Gaining the Economic and Security Advantage for the 21st Century:

A Strategy Framework for Electromagnetic Spectrum Control

LCDR J.D. McCreary
Electronic Warfare Directorate
Joint Information Operations Warfare Center
United States Strategic Command

31 August 2010

Acknowledgements

This report would not have been possible without the ongoing assistance and support from many people and organizations. The author recognizes the many individuals and organizations who volunteered their time and expertise throughout the course of this effort, and is extremely grateful for the input of the interviewees, including key current and former officials and personnel in government, industry, and academia. The methodology of using off-the-record, non-attribution interviews precludes the mention of participants by name, but we remain indebted to their generously giving of time and counsel.

In addition, the author would like to thank the principal organizations and individuals without whose support, this effort would not have been possible: Electronic Warfare Technology Task Force, co-led by Mr. Jaymie Durnan, Senior Advisor to the Principal Deputy, OUSD AT&L/DDRE, and Dr. Gerry Borsuk, Associate Director for Research, Naval Research Laboratory; Mr. Steve Callicutt, U.S. Strategic Command J8; Mr. Mark Johnson, SES, Director, Joint Information Operations Warfare Center; Col Hank Toussaint, USAF, Director, Electronic Warfare Directorate; Ms. Paige Atkins, SES, Director, Strategic Planning and Information Directorate, DISA; Defense Spectrum Organization; and Joint Spectrum Center. Finally, we are extremely appreciative of the research, writing, technical, and administrative support from Mr. John Alden and the rest of the ITT and Freedom Technologies, Inc. teams.

This page intentionally left blank.

EXECUTIVE SUMMARY

In this century, the electromagnetic spectrum (EMS) represents an unparalleled opportunity to leverage U.S. intellect and technology into greater knowledge, prosperity and security for the nation. There is an urgent need, however, to establish a comprehensive national EMS control strategy that will allow the United States to gain and sustain global competitive advantages that will benefit the United States militarily, scientifically, and economically.

EMS Control. EMS control enables freedom of action across all domains (land, sea, air, space and cyberspace), across the full Range of Military Operations (ROMO), (including deterrence, stability and/or humanitarian assistance operations, irregular warfare and major combat operations), and throughout all phases of operations. Not only is it clear that EMS control is essential to each of the six warfighting functions as shown in Figure 1 below [1], but there are obvious parallels to public/private sector functions in terms of safety, transportation, critical infrastructure, remote earth sensing, logistics, financial and medical networks and applications – just about any daily "operation" that one can think of at home, school, or work.

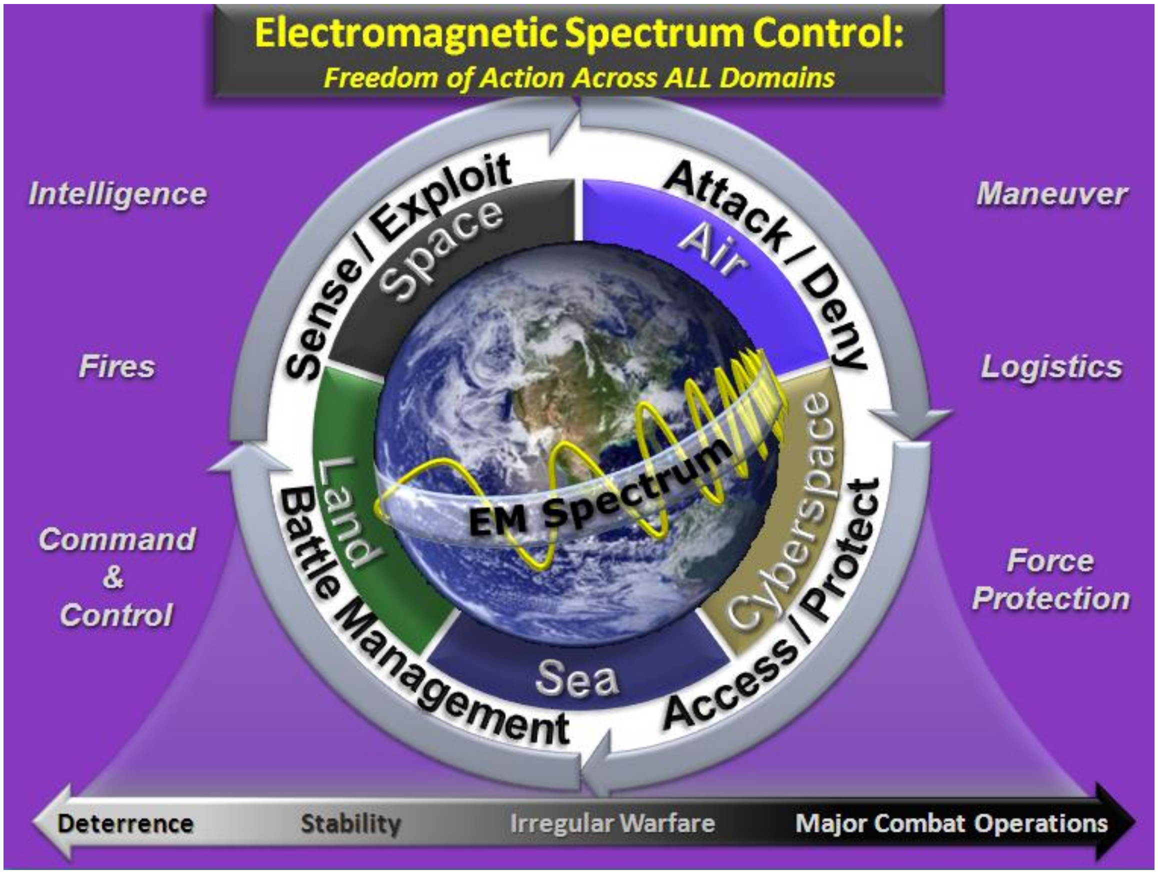


Figure 1. Electromagnetic Spectrum Control: Freedom of Action Across All Domains

Dual Use Technologies. Throughout the Cold War period, the United States led the field in pioneering dual-use technologies that relied on EMS. With the decline and collapse of its Soviet adversary, however, the United States lost the impetus to master and control the overall EMS technology space. This has impacted American military preparedness and effectiveness, because the underlying chipsets and other components that can advance spectrum-dependent military capabilities are now increasingly being developed in commercial research facilities – and those facilities are increasingly overseas. It is also an issue for national economic success and the competitiveness of U.S.-based high-tech manufacturing.

EMS Whole-of-Government Approach. A whole-of-government[1] approach will be required to redefine America's objectives for EMS control and technology leadership. This approach advocates the creation of a broad partnership between government and industry to create the conditions for innovation in underlying EMS-related technologies – as a national imperative.

Opportunities and Risks. The evolution of dual-use technology toward a globalized, decentralized, and commercialized paradigm presents a major systemic challenge for the Department of Defense (DoD). The U.S. military is increasingly dependent on spectrum, and the technological components of EMS-dependent systems, for a range of uses – from sensors and radars, to precision guidance systems, jammers, radio-frequency identification (RFID), ballistic missile defenses, avionics systems, satellite-based sensing, tracking of transport assets, and a host of others. Moreover, this profusion of systems is replicated in civilian uses, from weather satellites to remote store-and-forward utility data systems, public safety communications systems, and tracking of shipping containers. The national interest is now grounded firmly in the underlying technologies that harness EMS for these uses. Spectrum is an essential component of critical infrastructure, as well as of commercial competitiveness in mobile services, computer networking, and the myriad hand-held devices that light up tech news headlines. The U.S. military's EMS maneuver space is more and more constrained by factors such as weaponized commercial-off-the-shelf (COTS) technologies fielded by adversaries, as well as the commercial standards, policies, and manufacturing decisions of a globalized industry as shown in Figure 2.

[1] The term *whole-of-government* approach refers to an inter-agency approach that coordinates action across multiple departments and agencies of government. Leadership may be provided by one department, such as the Department of Defense, with White House coordination leading to complementary effective action by other departments such as Department of Homeland Security, Office of the U.S. Trade Representative or the National Science Foundation, and departments and agencies of government.

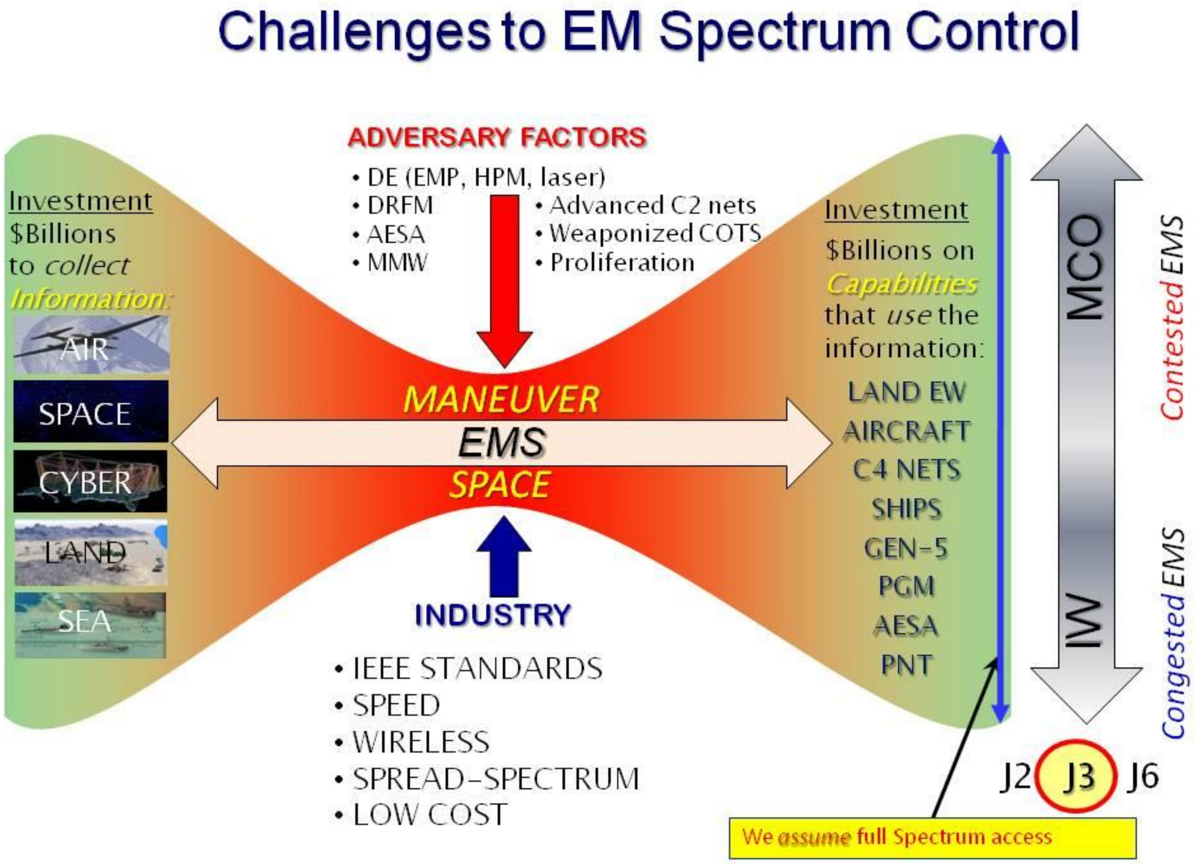


Figure 2. Challenges to EMS Control

The risk is not only that the United States is losing EMS control in absolute terms, but it might also lose its advantage in relative terms. The United States has an opportunity, however, to utilize the continuing strengths of its knowledge and industrial base. The Department of Defense must seize this opportunity to articulate, advocate, and participate in implementing a high-level, comprehensive EMS control strategy for the 21st century. It must regain and maintain leadership in, and control of, the EMS environment at all levels of the value chain, from basic scientific knowledge through technology development, acquisitions, training, and operations.

Department Task Force Findings and Recommendations. The Under Secretary of Defense For Acquisition, Technology, and Logistics' Director, Defense Research and Engineering's Electronic Warfare Technology Task Force (EWTTF) performed a ground-breaking outreach effort that resulted in a number of findings and recommendations. This group proactively reached beyond current thought patterns, stereotypes, and traditional military-industrial relationships to engage commercial technology leaders in a dialogue about EMS-related technology development, adoption, and dissemination. The EWTTF concluded that the United States must coordinate national action to sustain American leadership – both military and economic – into the 21st century. The EWTTF's research resulted in several major findings regarding the EMS technology development environment:

- The U.S. is no longer the dominant force in the development of EMS component technologies, which are increasingly produced offshore by a globalized industry of U.S. and non-U.S. manufacturers;

- The technical knowledge base that serves as a foundation for innovation also is increasingly globalized, allowing the outsourcing of intellectual capital beyond U.S. shores;

- The U.S. military's ability to instigate and nurture EMS technology research and development is far exceeded by the rapidly expanding human and financial resources of the global commercial world;

- The U.S. military acquisition process is over-burdened and insufficiently flexible, engendering a slower pace of technology adoption than is required;

- Private sector actors, and related academic and research entities, often are willing to engage with the military in a dialogue on constructive solutions to EMS challenges;

- Both government and industry must nurture and sustain a "culture of innovation" in order to enhance and accelerate the delivery of new technologies; and

- Government and industry face challenges associated with the quantity and quality of available data and the means to effectively and efficiently analyze, assess, and mine both structured and unstructured data.

Recommendations of the EWTTF included the following:[2]

- DoD must recognize, at a strategic level, the primacy of EMS and wireless technologies among the foremost shapers of today's operational environments.

- As a nation, the United States must fundamentally broaden the scope of public-private collaboration to revitalize and expand the country's intellectual and industrial base for EMS technology.

- DoD should implement clear, strong, and high-level leadership to address the breadth and scope of tactical, operational, strategic, procedural, and organizational issues involving EMS, which cut across current internal lines.

- DoD must participate in articulating and implementing a national strategy, involving government, industry and academia, to create an EMS environment that works holistically to promote knowledge, prosperity, and security.

[2] This paper focuses on primarily non-technical issues in an effort to create a strategic framework for addressing public/private/government spectrum-related issues. A separate classified EWTTF report focused on DoD-specific needs as tasked by the Honorable Zachary Lemnios, Director, Defense Research and Engineering [2].

- This strategy should recognize, as its foundation, the decentralization, globalization, and rapidly compressing timelines of EMS technology development.

- DoD should recognize and leverage the irreversible shift toward consumer demand and commercial interests as the primary drivers of technology innovation, supplanting the former role of military program development.

Implementation of a National EMS Strategy. How does the United States proceed to develop a comprehensive, national EMS strategy? Any such strategy must involve multiple agencies within government, as well as all industries that employ EMS to produce goods and services. Moreover, it must address the needs and requirements of all stakeholders through win-win solutions and approaches, avoiding zero-sum-game decision-making that picks winners and losers. Finally, it has to be results-driven, keeping in mind the need for competitiveness and innovation at all levels, from the tactical to the strategic – from the PDA to the polar-orbit satellite. Key principles include:

- Recognizing the prime importance of EMS;
- Recognizing the ongoing strengths of US technological capabilities;
- Recognizing the leading role of commercial technology development;
- Recognizing the need for a whole-of-government approach; and
- Recognizing the opportunities for public-private partnerships.

With these principles in mind, it is now possible to apply a model for development of that strategy. The goal is to build a national EMS strategy, for both national and international implementation, based on:

- Identification of assumptions;
- Assessment of realities;
- Listing of objectives;
- Analysis of the instruments of power/influence (policy, diplomacy, economics, force, etc.);
- Gap analysis: what instruments of power/influence must be developed to reach national/international objectives.

Another way to envision the development of a strategy is through a model involving the following elements in a "value chain" as shown in Figure 3:

- **Basic research/academia/education –** This encompasses the basic technical knowledge engendered throughout U.S. society, by its institutions of education and research.
- **Science and technology R&D –** This includes the universe of resources and activities devoted to focused science and technology research and development (S&T R&D).
- **Technology prototypes –** The shift from pure, or even applied, engineering to product development is one of the chief areas where commercial technology providers excel relative to military counterparts.
- **Targeted development and rapid acquisitions –** The U.S. military must be able to respond rapidly, with efficient allocation of resources, to immediate threats and new definitions of requirements. Experimentation will play a key role here.

- **Training, Education, Test & Evaluation, and Exercises –** Every good organization, DoD or otherwise, needs to understand what the emerging environment means in terms of threats and opportunities to its mission. Some of this requires intellectual enlightenment, and some of it comes from examining real-world effects before significant resources are invested and operational assumptions are made.
- **Operational Deployment –** This involves translating national EMS-control strategies into both security and economic environments and their commensurate operations, along with feedback and implementation "lessons learned" that inform other elements in the cycle.

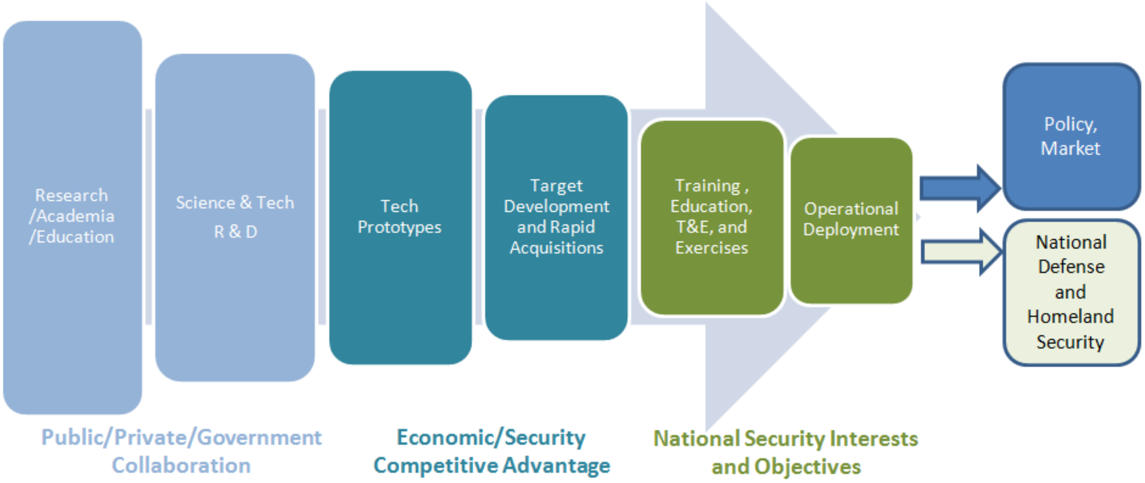

Research /Academia /Education
Science & Tech R & D
Tech Prototypes
Target Development and Rapid Acquisitions
Training , Education, T&E, and Exercises
Operational Deployment
Policy, Market
National Defense and Homeland Security
Public/Private/Government Collaboration
Economic/Security Competitive Advantage
National Security Interests and Objectives

Figure 3. Value Chain Development Strategy

Steps to Build Consensus. In order to realize these models, a whole-of-government and public-private approach will be necessary. This will depend upon institutions and agencies beyond the scope or authority of the DoD. Leadership within the Department can, however, have a catalytic effect upon the remainder of government and private industry. Steps in building a consensus around a new national EMS strategy could resemble the following:

Step One: Build consensus around DoD leadership.

Step Two: Coordinate with high-level Executive Branch leadership.

Step Three: Identify an appropriate forum for public-private partnership

Bottom Line. In order to secure both national prosperity and national security, the United States must undergo a paradigm shift in attitudes, policies, process, and structure with regard to dependence on and ability to control the EMS. The core of this paradigm shift is the mutual recognition, in both government and commercial entities, that revitalization of the Department’s ability to serve as an engine and consumer of commercial EMS technology is vital to the achievement and sustainability of American pre-eminence in this sector. The Department cannot achieve this by itself; it requires a whole-of government approach, both supporting and receiving support from U.S. and global industry. DoD must be part of the mainstream in developing and fielding technology in order to keep pace with it. DoD must lead the way in developing a new national consensus and strategy for capitalizing on America's intellectual and technological advantages. The United States must, and will, employ all of its resources to regain leadership in the EMS sphere, benefiting all of its citizens and its allies and leading the world toward a more prosperous, productive, and peaceful future.

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

1. INTRODUCTION

Electromagnetic spectrum (EMS) control and related technologies have become fundamentally important to national security and prosperity. Increasingly, those technologies are blurring the lines between commercial and military applications. In a world that is becoming both wholly connected and increasingly mobile, EMS is a primary enabler for future military, economic, and social development.

1.1 BACKGROUND

Over the past several months, a high-level EWTTF has been reaching out to commercial companies to better understand how cutting-edge commercial innovators maintain their research, development and implementation leadership in today's complex marketplace. The effort, coordinated through the Joint Information Operations Warfare Center at U.S. Strategic Command (USSTRATCOM), is designed to facilitate a broad discussion between key leaders of the high-tech industries in the United States and the Department of Defense (DoD) regarding electromagnetic spectrum-related aspects of EW.

The following leaders have addressed in simple terms the importance of EMS control:

> *"Whoever controls the electromagnetic spectrum on the battlefield will win the next war." -- Admiral Sergei Gorshkov, former Commander of Fleet, Soviet Navy, 1956*
>
> *"The side that seizes electromagnetic superiority is the side that will have the combat initiative." -- Major General Yuan Banggen, Peoples Liberation Army, China*
>
> *"I'm hoping we treat spectrum as a scarce renewable resource which should be used for the common good of the consumer and to make available the most innovative devices that can connect to those consumer."-- Google founding board member Ram Shriram*

EMS and allied technologies have become fundamentally important to both national security and national prosperity. Increasingly, those technologies are blurring the lines between commercial and military applications. Consider:

- Insurgents in Iraq and Afghanistan have used simple consumer devices, such as keyless entry fobs and garage-door openers, to trigger improvised explosive devices (IEDs) that have killed and maimed U.S. soldiers;

- China has demonstrated the ability to shoot down a satellite, instantly calling into question not only the strategic remote sensing, intelligence-gathering, and communications capabilities of every other military, but all kinds of critical remote sensing systems needed for scientific purposes;

- U.S. military pilots are reporting for duty – in Nevada – to pilot aircraft over the skies of Afghanistan and Pakistan, using Global Positioning System (GPS) and other spectrum resources to attack insurgents – the same GPS satellites that allow motorists to navigate or summon help to their automobiles;

- Wireless sensing networks are being designed and implemented, with dual-use technologies, to collect real-time data on materials stresses in bridges and other critical infrastructure, or to remotely monitor environmental contamination or individual patients' vital signs and medical conditions;

- The same underlying monitoring technologies can be used to chart battlefield movements, the health of astronauts, or to track military logistics operations.

In a world that is becoming both wholly connected and increasingly mobile, EMS is a primary field for future military, economic, and social development. The building blocks of this development are the chipsets, antenna arrays, lightweight materials, rare metals, long-lived batteries, and digital signal processors that underlie everything from portable gaming systems to RFID tags and ground-penetrating radars.

The universe of EMS-related components and devices has become a battlefield – not just figuratively, but literally. Already, in the first decade of this century, the United States has fought wars not only in the streets, plains, and mountains of Afghanistan and Iraq, but through the radio waves that connect them. Spectrum has been used to attack, defend, observe, and hide from the enemy. Unlike in previous conflicts, electronic warfare (EW) is now increasingly linked to civilian equipment and infrastructure, non-military uses, civil governance, and daily life. There is no intrinsic difference between a radio frequency that is used to make a phone call and one that is used to detonate an IED. Similarly, the groundbreaking technology advancements that make components smaller and more efficient can drive both commercial and military capabilities.

1.2 OBJECTIVE

The overall objective is to analyze and discuss the output of the EWTTF effort, and frame a concrete strategy for implementing improvements to DoD spectrum management, acquisitions and operational policies and doctrine.

The Department’s Director, Defense Research and Engineering, established the EWTTF on 28 September 2009. The EWTTF discussed all aspects of EMS, EMS control, and related technologies. They also interviewed major manufacturers and developers of wireless communications and technologies that use the spectrum. Based on these discussions and interviews, the EWTTF arrived at a number of findings and conclusions. Based on the EWTTF efforts, this report addresses the requirement for and an approach to establish an EMS national strategy to meet the overall objective above.

The parameters of EMS control include economic, political, and security aspects as they have developed in the first decade of this century. There is a need for a national EMS strategy that considers these aspects. The Department needs to examine the EMS issues and summarize the current realities. The result will be a definition of comprehensive EMS control, ranging from the counter-IED effort all the way up to the national policy-making level. Ways in which such a national EMS strategy should address current gaps and issues will be explored. Finally, the report will discuss the framework for a national EMS strategy, based on a national approach that recognizes and leverages current civilian pre-eminence in spectrum-based technology development and deployment.

2. OPPORTUNITIES AND RISKS

The evolution of dual-use technology toward a globalized, decentralized, and commercialized paradigm presents a major systemic challenge for DoD. The U.S. military is increasingly dependent on spectrum, and the technological components of EMS-dependent systems, for a range of uses – from sensors and radars, to precision guidance systems, jammers, RFID, ballistic missile defenses, avionics systems, satellite-based sensing, tracking of transport assets, and a host of others. Moreover, this profusion of systems is replicated in civilian uses, from weather satellites to remote store-and-forward utility data systems, public safety communications systems, and tracking of shipping containers. The national interest is now grounded firmly in the underlying technologies that harness EMS for these uses. Spectrum is an essential component of critical infrastructure, as well as of commercial competitiveness in mobile services, computer networking, and the myriad hand-held devices that light up tech news headlines.

The risk is not only that the United States is losing EMS control in absolute terms, but it might also lose its advantage in relative terms. Other countries can be expected to have closely monitored and studied the international development of EMS technologies. There is evidence that the governments of China and Russia, for example, have long perceived the strategic economic and military importance of EMS control. They already have based their force structuring decisions on the new reality that the critical mass of resources for research, education, training, and development has shifted decisively away from military applications and toward commercial ones. This allows them to invest billions of dollars in the kinds of dual-use technologies that underpin their advantages in both commercial and military equipment.

The United States has an opportunity, however, to utilize the continuing strengths of its knowledge and industrial base. The growing technological parity among companies around the world will continue to drive competition, and thus innovation. In embracing this mindset and culture of innovation, the U.S. can ride this wave of disruptive change, determining the future of dual-use technology, rather than being left behind in a technological cul-de-sac.

The Department of Defense must seize this opportunity to articulate, advocate, and participate in implementing a high-level, comprehensive EMS control strategy for the 21st century. It must regain and maintain leadership in, and control of, the EMS environment at all levels of the value chain, from basic scientific knowledge through technology development, acquisitions, training, and operations. At stake are the future lives of our soldiers, sailors, airmen, and marines, the success of U.S. military missions, and in fact, the broader future prosperity and security of the American people and the global community.

In light of the potential dual role of EMS related technologies as articulated above, further consideration and assessments will have to be made in the development of these technologies to ensure both national security and economic growth is addressed simultaneously. The next section investigates relationships in government between national security and economic or commercial concerns and the potential need for new policy that could maximize EMS-related technologies in both areas of concern.

3. MAKING SENSE OF AN INTERCONNECTED WORLD

In the United States, as in most developed countries, deeply rooted cultural and institutional traditions tend to establish firewalls – in terms of policy, regulation and psychology – between civilian and military spectrum usage. This properly reflects the pre-eminence of civilian governance and the largely de-militarized nature of contemporary life, particularly in developed democracies. Most civilians do not think of the airwaves around them as potential battlespace, or the technologies that empower texting as the same ones that can be weaponized to produce explosions or espionage. Nor do military officials typically encourage those realizations.

The risk is that in pursuing policies designed to maximize EMS-related technologies as an engine for prosperity, governments may lose sight of the crucial role that EMS technology also plays in guaranteeing the security that enables such prosperity. There is a risk that the critical mass of resources for research, education, training, and development will shift decisively away from military applications, isolating the security aspects of spectrum-dependent technology.

The United States has the opportunity to leverage its enormous spectrum technology assets into a strategic vision that correspondingly could enhance both national security and economic/commercial growth. Other economies – including those of rapidly developing countries such as China – will not be blind to this opportunity. For example, it is widely known that China couples a force-structure emphasis on EMS control with a comprehensive national economic, social, and political strategy to seek, obtain, and maintain technological leadership in all facets of EMS technology. The Chinese view military and economic strength as a seamless, synergistic whole, with good reason. The society that best organizes itself to leverage technology for knowledge, prosperity, and security, holistically, will determine its own fate in the rapidly expanding EMS environment.

The global environment that the United States faces was summed up in a description of transnational forces and trends contained in the 2009 National Intelligence Strategy document:

> Rapid technological change and dissemination of information continue to alter social, economic, and political forces, providing new means for our adversaries and competitors to challenge us, while also providing the United States with new opportunities to preserve or gain competitive advantages. [3]

As one can see, it is imperative that the national interest focus on coming up with a national EMS strategy if the United States wants to take advantage of the opportunity delineated above. The next section addresses the need for this national EMS strategy.

4. NEED FOR A COMPREHENSIVE NATIONAL EMS STRATEGY

The *EMS* environment must encompass reality at multiple levels – from the tactical to the national. It ranges from advanced jamming capabilities and counter-IED patrols, all the way up to the overall governmental and industrial structure of policies and market players that constitute a nation's reservoir of technology. This new era demands a comprehensive overarching whole-of-government view of EMS-related technology development that would ensure that: 1) both national security and economic/commercial growth are addressed in concert; and, 2) a national strategy is developed to control the EMS to meet both national security and economic goals. The national EMS strategy must also include the control of the EMS environment.

Control of the EMS environment enables freedom of action across:

- all domains (land, sea, air, space, and cyberspace),
- the ROMO, (including deterrence, stability and/or humanitarian assistance operations, irregular warfare, and major combat operations), and
- throughout all phases of operations.

Not only is it clear that control of the EMS environment is essential to each of the six warfighting functions shown in Figure 4, but there are obvious parallels to public/private sector functions in terms of safety, transportation, critical infrastructure, remote earth sensing, logistics, financial and medical networks and applications. This is also true for just about any daily “operation” that one can think of at home, school or work.

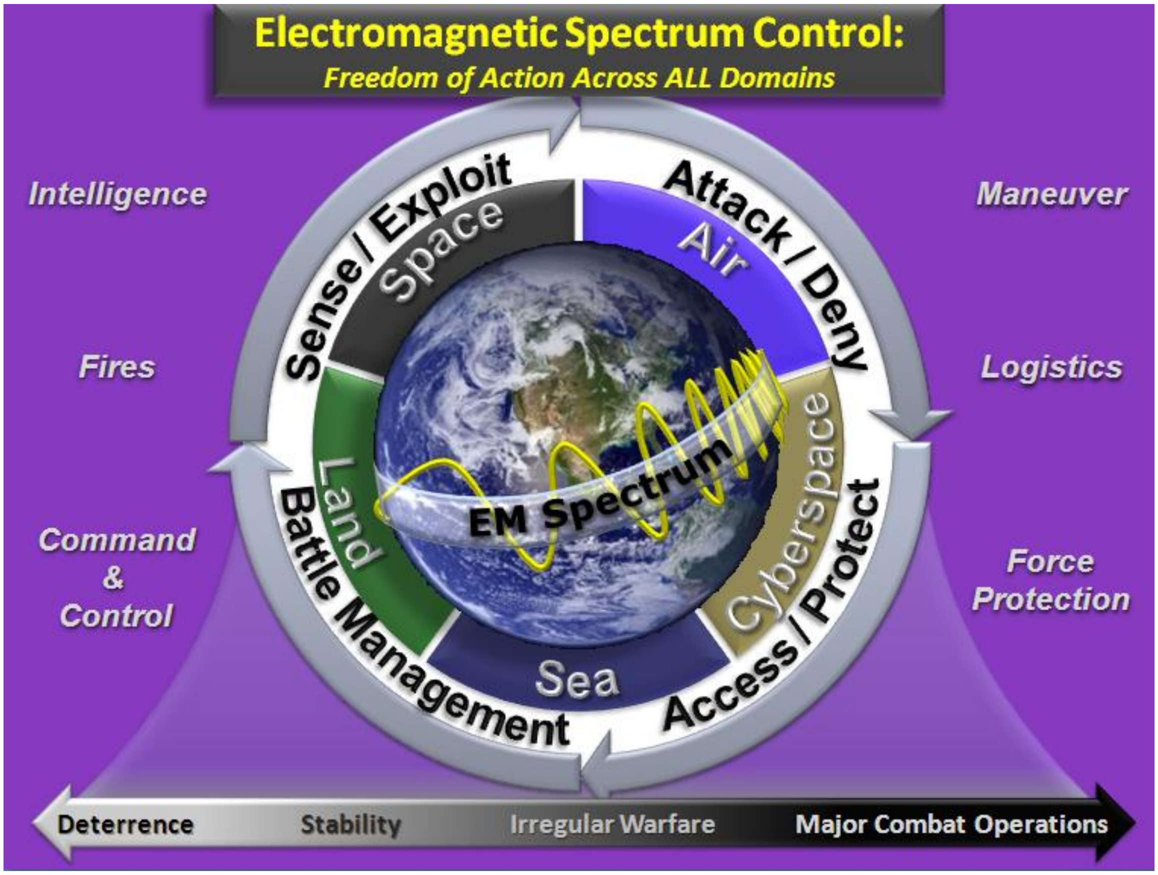


Figure 4. EMS Control [1]

The U.S. military is increasingly dependent on spectrum and the technological components of EMS-dependent systems for a range of systems, from sensors to radars, to precision guidance systems, jammers, RFIDs, ballistic missile defenses, avionics systems, satellite-based sensing tracking of transport assets, and a host of other uses. Moreover, this profusion of systems is replicated in both the absolute number and the large variety of civilian uses. The deployment of these communication systems will increase the complexity of the interactions within and between the military and civil sectors making it all the more important to control the EMS environment.

Increasingly, commercial drivers dominate the development of core components that go into everything from battlefield radars to baby monitors. Not surprisingly, adversaries seeking to wage asymmetric war have learned how to weaponize the underlying technologies and to take advantage of the constrained and chaotic nature of the EMS environment. As a result, U.S. and Coalition warfighters face threats that stem from hostile use of dual-use technology that is being developed beyond DoD control. In contrast to the historical situation, in which the *military* pioneered dual-use technology, the Department is now increasingly tied to multi-year spiral development programs that cannot keep pace with the rapid, competition-fueled commercial technology cycle. The U.S. military's EMS maneuver space is more and more constrained by factors such as weaponized commercial-off-the-shelf (COTS) technologies fielded by adversaries, as well as the commercial standards, policies, and manufacturing decisions of a globalized industry as shown in Figure 5. Constraining EMS use will have a very adverse effect on military communications.

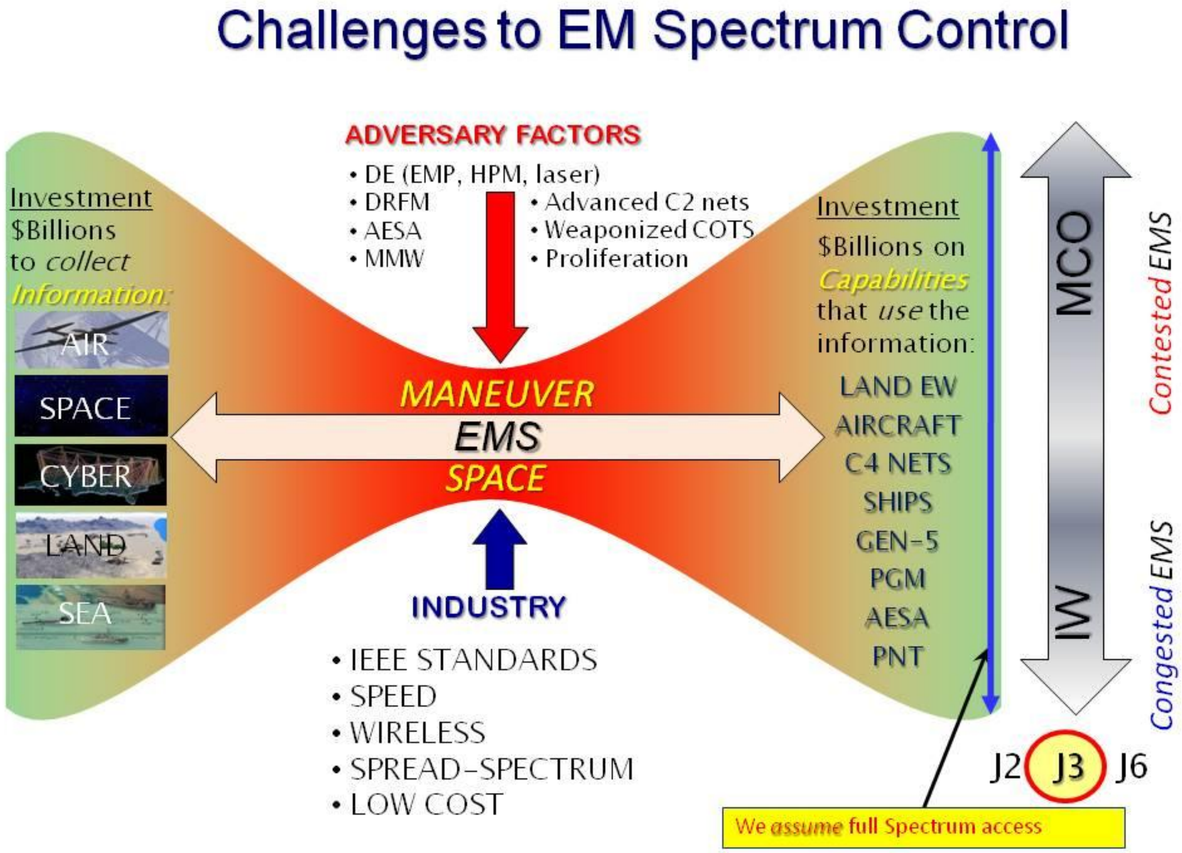


Figure 5. EM Spectrum Control

To alleviate the pressures on EMS access, and to inaugurate advances in underlying, dual-use technologies, the DoD must seize this opportunity to articulate, advocate, and participate in implementing a high-level, comprehensive EMS strategy that addresses the dual role of EMS related technologies and the control of the EMS environment in the 21st century at all levels of the value chain (Figure 3), from basic scientific knowledge through technology development, acquisitions, training and operations. At stake are the future lives of United States and Coalition soldiers, sailors, airmen and marines, the success of U.S. military missions, and in fact, the broader future prosperity and security of the American people and the global community.

The criticality of the EMS and the control of the EMS environment was addressed by the EWTTF established by the Director, Defense Research and Engineering on 28 Sept 2009. The next section will address the findings and recommendations of the EWTTF.

5. EWTTF FINDINGS AND RECOMMENDATIONS

The experiences and expertise gained by U.S. military EW specialists globally over the past decade have provided extraordinarily valuable lessons and insights into the nature of contemporary EMS use and EMS technology adoption throughout the conflict chain and across all aspects of civilian and military activities. These experiences were gained not only in Afghanistan and Iraq and Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF), but through monitoring the conflict in Georgia, stability operations in the Balkans, HA/DR operations in the U.S. Pacific Command (USPACOM) region, counter-narcotics operations, etc. These experiences prompted a re-examination of current assumptions about U.S. dependence on and ability to control the EMS, inclusive of strategies, policies, S&T, R&D, acquisition, test and evaluation, fielding and operations, as well as the supporting industrial and intellectual base. The result was the establishment of the EWTTF to examine the criticality of EMS in the battlespace and throughout the U.S. military value chain. The EWTTF initially held a symposium and met with representatives of DoD entities and defense industry representatives. Then, acknowledging gaps in the information, the EWTTF decided to expand its review to include input from technology players beyond the defense community. Interviews were held with representatives of U.S. and multinational telecommunications and information technology companies, other government agencies (such as the National Science Foundation), and academia. Details on the interviews can be found in Section 7 and the list of entities interviewed is shown in Appendix A.

The EWTTF discovered that the current U.S. military stance on EMS – particularly with regard to acquisitions – is out of synch with global realities. Acquisition of spectrum-dependent equipment is reliant on an outdated prime-contracting model that frequently results in cost overruns and delays, and that is unable to keep pace with technology trends. Moreover, the cross-cutting primacy of spectrum as a mode of operation has been largely under-valued by a Department that has emphasized the wired aspects of net-centric operations, while insufficiently appreciating the fast pace of development of the wireless systems that will better characterize the 21st century operational environment.[3]

The major findings of the EWTTF's research are as follows:[4]

- The U.S. is no longer the dominant force in the development of EMS component technologies, which are increasingly produced offshore, by a globalized industry of U.S. and non-U.S. manufacturers; [4]

- The technical knowledge base that serves as a foundation for innovation also is increasingly globalized, allowing the outsourcing of intellectual capital beyond U.S. shores;

- The U.S. military's ability to instigate and nurture EMS technology research and development is far exceeded by the rapidly snowballing human and financial resources of the global commercial world;

[3] As an example of the under-valuation of spectrum in strategic DoD thinking, the 2010 Quadrennial Defense Review (QDR) makes no mention of electromagnetic spectrum, nor does it mention the terms *radio-frequency* or *wireless*. By contrast, there are nearly 50 references to networks and cyberspace. The word satellite is mentioned only three times, and while there are more references to unmanned aircraft systems (16), none of them address spectrum access issues that should be addressed to ensure throughput and high bandwidth. *See Department of Defense, Quadrennial Defense Review Report, Washington DC, February 2010.* available at *http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf*.

[4] As previously noted, this paper focuses on primarily non-technical issues in an effort to create a strategic framework for addressing public/private/government spectrum-related issues. A separate classified EWTTF report focused on DoD-specific needs as tasked by the Honorable Zachary Lemnios, Director, Defense Research and Engineering [2].

- The U.S. military acquisition process is over-burdened and insufficiently flexible, engendering a slower pace of technology adoption than is required;

- Private sector actors, and related academic and research entities, often are willing to engage with the military in a dialogue on constructive solutions to EMS technology challenges;

- Both government and industry must nurture and sustain a "culture of innovation" in order to enhance and accelerate the delivery of new technologies; and

- Government and industry face challenges associated with data analysis, assessment, and mining, as well as structured versus unstructured data.

In addition, the broader dialogue throughout the U.S. government has focused the policy balance in favor of commercial uses of spectrum at the potential risk of national security aspects of spectrum. [5] The de-emphasis of spectrum as a vital component of military readiness is reflected in the stance of industry and the public, which generally remain ignorant of, or reluctant to acknowledge, the large and growing Defense requirements for EMS access. There is, in fact, a large and widening delta between civilian and military perceptions of spectrum opportunity and risk, in which EMS policy is falsely reduced to a zero-sum contest over “spectrum bands” and allocation decisions – to the detriment of the nation as a whole.

Meanwhile, the focus has shifted away from core and dual-use technologies – the basic components of sensors, radars, transceivers, and other equipment that drives both military and commercial capabilities. Those technologies are now predominantly developed for commercial use, and the resulting marginalization of military priorities – both within the Federal government and in overall society – poses a long-term threat to national security.

Based on these findings, the specific recommendations of the EWTTF are:

- DoD must recognize, at a strategic level, that EMS and wireless technologies are among the foremost shapers of today's operational environments.

[5] A review of hearings held, to date, by the 111th Congress, for example, is instructive regarding the current commercial inclination of spectrum policy in the Federal government. The House Committee on Energy and Commerce has held at least six hearings that are directly or indirectly related to spectrum issues – including on legislation or government initiatives (e.g.., the FCC’s National Broadband Plan) that could directly impact the access of Executive Branch agencies (including U.S. military units) to spectrum. Out of nearly 40 witnesses in those hearings, only one witness represented any Executive Branch department (Agriculture), and there were no DoD witnesses. Similarly, in the Senate’s Commerce, Science and Transportation Committee (which handles companion legislation), there have been three spectrum-related hearings, with no Executive Branch witnesses. In both the House and Senate, a large number of witnesses represented industry – and many industry groups (i.e., CTIA) were represented in multiple hearings. Moreover, the congressional committees that exercise jurisdiction over DoD -- House and Senate Armed Services, as well as Homeland Security and Government Reform in the Senate and Oversight and Government Reform in the House – have not addressed spectrum issues. This imbalance comes at a time when both the Federal Communications Commission and the administration are proposing major sharing or reallocation of spectrum access from government to commercial use. At this critical juncture, the Department of Defense has been essentially silent in Congress on the potential impact to military operations of this proposed sharing or reallocation.

- As a nation, the United States must fundamentally broaden the scope of public-private partnership to revitalize and expand its intellectual and industrial base for EMS technology, bolstering knowledge, prosperity, and security.

- DoD should have clear, strong and high-level leadership to address the breadth and scope of tactical, operational, strategic, procedural and organizational issues involving EMS technology, which cut across current internal lines.

- DoD must participate in articulating and implementing a national strategy, involving all of government, industry and academia, to create an EMS technology development environment that works holistically to promote knowledge, prosperity, and security.

- This strategy must recognize, as its foundation, the decentralization, globalization, and rapidly compressing timelines of EMS technology development.

- DoD must recognize and leverage the irreversible shift toward consumer demand and commercial interests as the primary drivers of technology innovation, supplanting the former role of military program development.

The next section provides the context for the Department's examination of EMS issues and summarizes the current realities that result in a definition of the comprehensive EMS environment, ranging from the counter-IED effort all the way up to the national policy-making level.

6. DOD'S EMS CHALLENGES AND OPPORTUNITIES

6.1 DOD'S OPERATIONAL CONTEXT

DoD has an unique opportunity to shape, use, and anticipate emerging technologies in a contested and congested EMS environment. As "21st Century Electronic Warfare," a review of EW in the Information Age, noted: "In the 21st Century, the Diplomatic, Informational, Military, Economic & Law Enforcement elements of national power will operate in a global environment characterized by socio-economic interdependence, uncertainty, complexity, and continual change." In this environment, nations will rely on the use of EMS technology to "achieve strategic advantage and to strengthen the instruments of national power. [5] The United States can, and must, be a leader among those nations.

First, the U.S. must assess current realities. The pace of technological change of the past several decades has led to two divergent development paths:

(1) Wireless technology revolutionized and unified the commercial sector with open standards, flexible architectures, and rapid development cycles.

(2) At the same time, military efforts to seek EMS-based technological advantages were often fragmented by a reliance on stove-piped, multi-year spiral development of proprietary systems unique to the U.S. military industrial complex.

As a result of this dichotomy, DoD's ability to control the EMS technology environment has been eroded, at the potential risk to future U.S. Forces' operational capabilities. The National Military Strategy of the United States (2004) characterized deterrence as resting on an adversary's understanding that the U.S. "has an unquestioned ability to deny strategic objectives and to impose severe consequences in response to hostile or potentially hostile actions." A Defense Science Board (DSB) study cast such challenges in the context of "capability surprise," which is facilitated by globalization and technology. [6] DSB identified contributing factors as:

- **Adaptation of new technology**: Adversaries employ new, previously unused technology and adapt it to their needs; and
- **Rapid fielding**: Adversaries develop a new military capability via existing technology and transition to a fielded capability faster than expected.

DoD must progressively limit and then eliminate the risk of such "capability surprise" by adopting the rapid technology development cycles and adaptation that now characterize commercial development processes.

6.1.1 Origins of Change: Post-Cold War Through Desert Storm

There are two simultaneous trends that reduced U.S. military readiness to address EW threats:

> *Atrophy of Specialized EW Capabilities and Doctrine.* After the Cold War, the focus on EW counter-operations to respond to the Soviet threat was reduced. The Army, faced with a diminished need to maintain an expensive and highly specialized EW capability, divested itself of an asset that no longer seemed necessary. "Subsequently, combat formations were planned without taking into consideration EW requirements, no new EW doctrine was written for more than a decade and what was left of the Army's residual EW capability slowly atrophied to the point that it became ineffective… [B]y September 11, 2001, there was little EW capability to be had in the U.S. Army."[7]
>
> *Adversaries' Appreciation of U.S. Dependence on High-Tech Weaponry.* During Operation Desert Storm in 1991, extensive CNN coverage showcased the high-tech prowess of the U.S. military, including many capabilities that relied on spectrum. The U.S. was highlighting its emerging dependence on spectrum-based technological capabilities for a global audience. This happened just as Information Age technologies were becoming more readily accessible – and affordable – to nation-states and sub-national adversaries. Many of those adversaries noted the U.S. high-tech capabilities and began to adjust and modernize their force structures and military doctrines to counteract them. The explosion of underlying, dual-use radio components generated tools that could be incorporated into their EW strategies.

The roots of the Department's current challenges with EMS technology adoption stem from a shift in emphasis away from EW at the end of the Cold War. The Soviet Union had posed a sophisticated EW threat to U.S. military forces, having incorporated what was then known as Radio-electronic Combat as an integral part of its military doctrine. [8] After the fall of the Berlin Wall, DoD shifted its budgetary and technology development resources elsewhere. This was the case, for example, with respect to military investments in Electromagnetic Pulse technology. [9]

The impact of the military's reaction to this threat reduction was long-lasting, with repercussions extending into the post-9/11 environment. DoD's Fiscal Year 1996 EW Plan noted: "Operation Desert Storm demonstrated the effectiveness of sophisticated weapons systems. Buyers around the world will use that performance as a yardstick for acquisition decisions." [10] The result was an asymmetric vulnerability in the U.S. ability to counter non-traditional EW threats. Adversaries developed sophisticated approaches with COTS technology, leveraging DoD's reliance on military systems that had less agility than mass-market devices.

6.1.2 Evolution of Commercial Technology on Modern Battlefields

As Operation Desert Storm was occurring in 1991, the commercial wireless revolution was just beginning to explode, giving rise to a global wave of spectrum-based technological innovation. The commercial technology world became more diverse and fragmented, with new developments flowing out of globally agreed standards and inexpensively produced infrastructure, devices and systems. Our adversaries took advantage of the dual-use capability and diversity of spectrum-dependent commercial technologies, developing the ability to fade into the background of civilian infrastructure.

Ten years later, OEF and OIF-1 presented a steep learning curve about adversaries' ability to adapt those dual-use commercial EMS tool sets to offset and bypass some military hardware. U.S. military acquisition strategies were compelled to respond rapidly to the COTS threat. But there is a high cost to reacting to operational realities, rather than driving and creating those realities in the first place. A strategic vision was needed to guide and support more proactive fielding of advanced equipment and tactics.

Complicating the operational environment, particularly in Iraq, was the initially extensive deployment of COTS systems – such as Worldwide Interoperability for Microwave Access (WiMAX) and Global System for Mobile Communications – facilitated by State Department civilian reconstruction efforts. Such efforts were critical to re-establishing a robust commercial infrastructure in Iraq, but they enabled insurgents to use private-sector networks as weapons and for command and control. There was an eventual moratorium placed on such COTS-based systems being deployed in the Phase 4 environment in Iraq. Essentially, the U.S. military found itself in a hostile environment defined by commercial technology it did not possess and for which it was not thoroughly prepared.

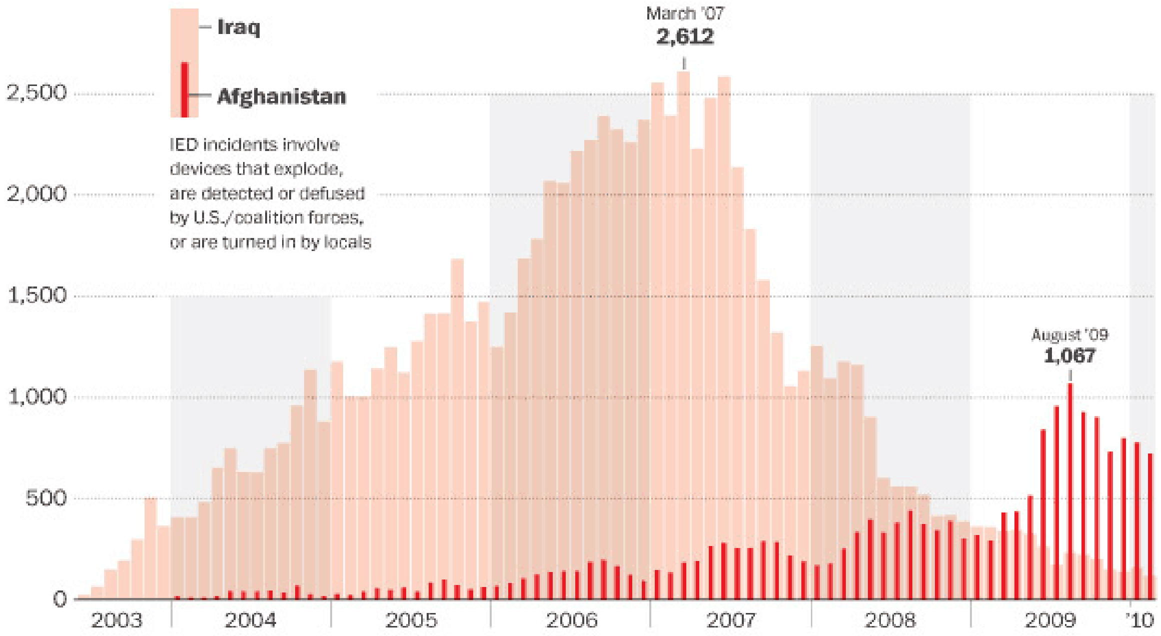
The implications for the future were immediately apparent. At an operational level, it is important to control the EMS environment during all of the six phases (0 through 5) identified in Joint Publication 3.0 (Joint Operations). If EMS control or advantage is lost at any phase of operations, it risks mission success at all other phases. Operational planning must be coordinated closely among the J2, J3 and J6 staffs. [7] Moreover, EMS environment control is crucial not only for

[7] In modern military staff structures, the numbers 2,3 and 6 refer to staff offices devoted to intelligence gathering, operations and communications, respectively. Wherever multiple military branches are represented (i.e., Army, Air Force, navy or Marines), the staff is described as "joint," and the numbers are preceded by the letter "J". Thus, a J3 office would be a joint operations office of a military staff. In the recent past, there have been problems stemming from: Lack of coordination among the EW-focused J2 and J3 staffs, and the spectrum-management operations of J6 staffs; over-emphasis on wireline communications within J6 planning and deployments, at the expense of due attention to EMS factors; absence of EMS control at multiple phases of conflict,

warfighting, but for stability operations, humanitarian assistance/disaster relief and other important military missions. Loss of EMS environment control, as a result of falling behind in technology adoption, therefore, can endanger all U.S. military missions, at all phases of activity.

The best-documented example of how the U.S. military has had to respond to "weaponized" commercial technologies involves IEDs. The Office of the Army Chief of Staff created an Army IED Task Force in 2003, reaching out to Army components, sister services, the private sector, and academia “to improve threat-intelligence gathering, acquire counter-IED (C-IED) technologies and develop C-IED training. This effort led to a reduction in casualty rates per IED attack despite an increased in-theater use of the devices. It then evolved into the establishment of a Joint IED Task Force that leveraged the expertise of warfighters across services. DoD Directive 2000.19E in 2006 converted the joint task force to a permanent entity – Joint IED Development Office (JIEDDO). JIEDDO established a Competitive Strategies Group in FY 2008 to develop and provide what it describes as a “a continuous competitive advantage in the C-IED fight by anticipating second and third order effects of adversary adaptation in the use of IEDs in order to defeat IEDs as weapons of strategic influence.” The Herculean efforts of JIEDDO to address counter-IED capability gaps points to the larger problem DoD faces: how to strategically and institutionally prepare to address rapid adaptation of dual-use components of non-military hardware.

As shown in Figure 6, the use of homemade bombs, or IEDs, has markedly decreased in Iraq, while their use in Afghanistan is soaring.



SOURCE: Joint Improvised Explosive Device Defeat Organization | The Washington Post - March 18, 2010

Figure 6. IED Incidents in Iraq and Afghanistan Since June 2003

Increasingly, military forces of other countries will have force-structured systems and policies to

beginning with Phase 0; and lack of awareness of the asymmetric threat presented by adversaries' use of the civilian infrastructure to engage in EMS-based warfare.

utilize the confusion and "cover" of non-military EMS-based systems to engage in electronic attack, electronic protect and EW support in highly sophisticated ways.[8] This is especially true after the experience of Coalition forces in Iraq and Afghanistan. The United States can expect that military leadership in other countries will leverage their nations' growing technological strengths – including EMS-based technologies – into military strengths that will match up well against the perceived vulnerabilities of their potential adversaries. Indeed, lessons in how EMS commercial technology is shaping the battlefield environment are emerging out of the conflict in Georgia, stability operations in the Balkans, humanitarian assistance and disaster relief operations in the USPACOM region, and counter-narcotics operations in U.S. Southern Command.

While none of these scenarios has yet yielded EW threats of a magnitude similar to those posed by the former Soviet Union, these experiences point to the potential of near-peer and, in the future, peer adversaries utilizing sophisticated dual-use technologies to leapfrog their own EMS environment control capabilities, particularly in anti-access and area denial scenarios. In the case of the Georgian conflict in 2008, for example, the Georgian government contended that Russia engaged in cyber warfare, by disabling Georgia's Ministry of Foreign Affairs Web site. [11] In addition, USPACOM planners are becoming increasingly aware of China's capabilities in the EMS technology arena. Of note, Chinese equipment has found its way into Afghanistan and Iraq, where it has been used by both the adversaries the U.S. is trying to defeat and the very economic, information, and security infrastructure that the U.S. is trying to support, further complicating U.S. and Coalition operations.

6.2 DIVERGENT PATHS: DOD AND CIVILIAN TECHNOLOGY DEVELOPMENT

6.2.1 EW, Spectrum Management and CNO

In recent years, an increased perception of threat to DoD operations has shifted the focus to the cyber-domain. Perhaps due to the emphasis on Net-Centric Warfare, the perception of asymmetric vulnerability was perceived primarily in the area of Computer Network Operations (CNO), rather than in terms of EW. The Department is working on a holistic approach to advance CNO and cyber-security, but it does not yet have such a strategy to achieve EMS control.

Within the civilian staff of the Office of the Secretary of Defense (OSD), spectrum issues are currently addressed by the Office of the Assistant Secretary of Defense for Networks and Information Integration (NII)/Chief Information Officer (the Spectrum Directorate), which is supported by the Defense Information Systems Agency's Defense Spectrum Organization (DSO), which includes the Joint Spectrum Center and the Strategic Planning Office. These organizations, however, primarily address *spectrum management* issues, which are discrete from EW *per se*. EW has often been separated from (and implicitly overlooked by) efforts to modernize and plan for

[8] Electronic attack includes both offensive and defensive use electromagnetic, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Electronic protect entails actions taken to protect personnel, facilities, or equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly capability. And electronic warfare support is the effort to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy, for the purpose of immediate threat recognition. See, http://www.fas.org/news/reference/lexicon/dee.htm#electronic warfare

improved spectrum management. In simple terms, until the IED threat, military spectrum management did not adequately embrace "commercial" spectrum use or fully comprehend the rapidly escalating adoption of dual-use technologies by non-traditional adversaries.

Moreover, while the CNO component of IO has attracted resources in recent years (a result of the emphasis on cyber-security), EW has lacked a strong DoD institutional advocate.[9] Absent a stable patron for EW – and with a lack of institutional leadership and management approaches – there has been a lack of focus on this dimension of IO, as military planners redirected resources and attention to CNO. The latter increasingly became synonymous with wired networks rather than spectrum-based infrastructure – for both communications and non-communications systems. A recent Congressional Research Service report noted: "[A]s high technology is increasingly incorporated into military functions, the boundaries between all five IO core capabilities are becoming blurred."

Meanwhile, the 2010 Quadrennial Defense Review (QDR) has begun to address the need to modernize related capabilities. Two elements of the QDR cite the need to "enhance the robustness of C4ISR" (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) and to "defeat enemy sensor and engagement systems" -- both of which are possible only through EMS control. [12] In addition, the QDR report affirms that "our enemies are adaptive and will develop systems and tactics that exploit our vulnerabilities." Without touching directly on EMS environment control, the report noted, "For example, IEDs have been used effectively against U.S. and other counterinsurgency forces, and have become the weapon of choice of some enemies. We must assume that the IED threat will evolve and persist even as better countermeasures are developed." Those countermeasures will include EW electronic attack aircraft designed to leapfrog enemy capabilities. Thus, the Department is now articulating the need to move ahead after decades of relative inattention to EMS control issues. Even so, the response is frequently still framed in terms of platform assets (i.e., aircraft) rather than in terms of an integrated EMS control strategy. [13]

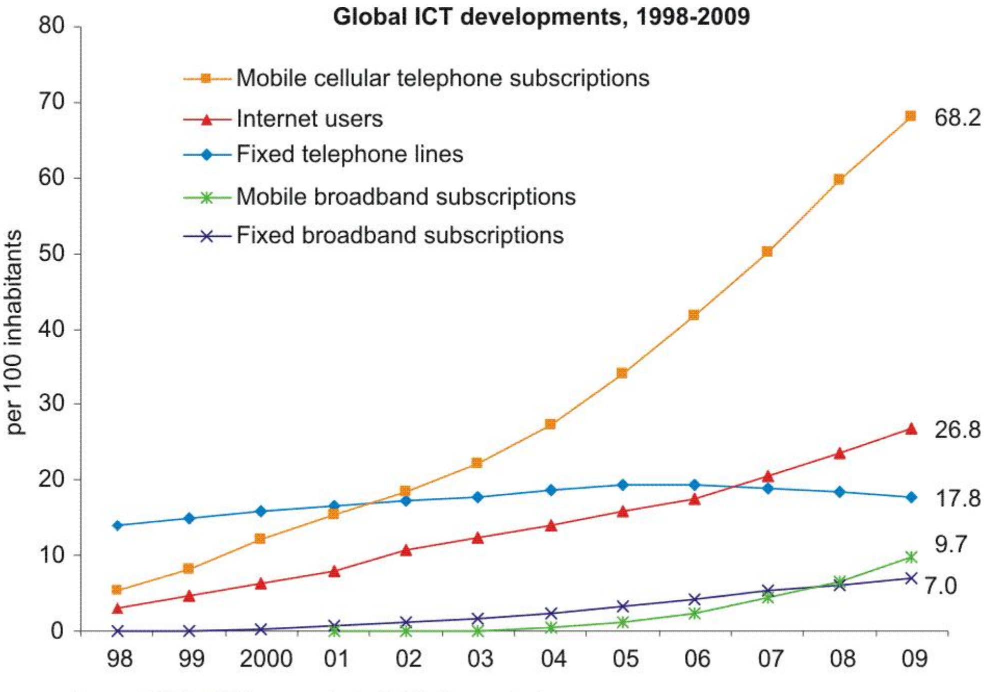
6.2.2 The Explosion of Commercial Technologies

Meanwhile, the relative de-emphasis on EMS within the Department was at odds with the wholly disruptive transformation of spectrum-based technology components that occurred in the commercial sector. Over the past two decades, the explosion of demand for, and development of, commercial EMS technologies (Figure 7) has overtaken DoD's role as an engine for U.S. technology pre-eminence. DoD no longer drives EMS technology development; its role has been superseded by an ecosystem of private sector or university-driven research, product development, standards-setting, and marketing.

Moreover, the geopolitical nature of the production of critical components has shifted. Until recently, global leaders in technology development have primarily been based in countries that were U.S. alliance partners – if they were not U.S.-based. Globalization, however, has radically altered the status quo, both in military and technological capabilities. Labor forces are

[9] As discussed in Section 3.4.2, JROCM 177-09 and the STRATCOM study on EW signified the identification of a military solution for the Department's leadership on EW. However, it is not yet clear how OSD will reorganize institutionally on the civilian leadership side to meet these challenges.

increasingly mobile and well-educated, and they can be tapped (through outsourcing) wherever they can be found and trained. EMS technology advances have freed innovation, knowledge, and data to become highly mobile and transferable. Increasingly, countries and non-state actors outside the traditional U.S.-friendly western alliance structure can and are developing and procuring highly critical and advanced EMS technologies, either through home-grown efforts or technology transfers – legal and illegal. A report by Informa Telecoms & Media Research revealed a "major reshuffle" in the world's major Intellectual Property (IP) rights holders from earlier generations of wireless technologies. Digital (2G) cellular technologies, as well as 3G and "3.5G" technologies, were powered by the licensed IP of Qualcomm, Nokia and Ericsson, all North American or European companies. While Qualcomm and Interdigital continue to control 19 percent and 20 percent of the patents for LTE (4G) technologies, to date, China's Huawei has surged to third position, with 9 percent, followed by Samsung, with 8 percent of patents. Nokia and Ericsson have slipped into a tie for fifth place, along with South Korea's LG. This shows a shift in the dominance of IP from West to East, with Qualcomm retaining an advantage based only on its early development of CDMA technology.



Source: ITU World Telecommunication/ICT Indicators database.

Figure 7. The Soaring Growth of Commercial Wireless Services

The spread of technological sophistication to newer market players, many of them based outside U.S. alliances, requires a re-examination of these governments' practices and motives. Unlike the western countries' practice of keeping military and industrial policies separate, countries in the Middle East and East Asia do not always adhere to a bright-line distinction. Rather, promotion of commercial technologies is seen as directly benefiting military readiness, and vice-versa. Whether the linkage is direct, through common government ownership and management, or whether it is indirect, through development of a common "prosperity-security industrial ecosystem," these countries are dedicated to finding mutual synergies between development of commercial and military technologies.

Some countries (e.g., China and Iran) are potential rivals or adversaries, while others (e.g. Israel or Singapore) are more likely to share similar interests and long-standing ties with the United States. They can provide models for how a country expresses and exerts national policy to realize national goals – without leaving either military or commercial competitiveness out of the mix. Thus, the U.S. increasingly exists in a geopolitical world that considers EMS technology development a strategic imperative, both militarily and economically – and takes deliberate steps to make sure dual-use technology supports improvements in both areas, simultaneously.

6.3 DOD'S EFFORTS TO DEVELOP AN EMS CONTROL STRATEGY

The creation of the EWTTF, under the auspices of OSD, represented a culminating response to the above-mentioned trends, which compelled DoD to focus on technological developments shaping the EMS environment with a comprehensive, holistic analysis. The Task Force has focused on critical questions, including "what is the required investment in technology?" and "what is the optimal technical environment?" Because responsibilities for EW – and in turn for EMS control – are fragmented across various parts of the military, everyone faces EMS challenges, but no single entity "owns" the solution set. A focused evaluation, which transcends the "lanes" of individual components and commands, was required to create a blueprint for proactively responding to the vulnerabilities created by technological, geopolitical, economic and international (e.g., export-import) and domestic (e.g., EMS) policy.

6.3.1 Activities in USPACOM/Briefing of JCS

In 2007, Admiral Timothy Keating, then-commander of USPACOM, provided a briefing to the Joint Chiefs of Staff (JCS) Tank on the impact of evolving EMS capabilities and the complex environment in USPACOM's Area of Responsibility. Working with General Kevin P. Chilton, USSTRATCOM Commander, PACOM EW leadership briefed General James E. Cartwright, JCS Vice Chairman. While Vice Chairman Cartwright indicated that the briefing had laid out a comprehensive *regional* perspective of the EW challenge, a *global* perspective was required, which General Chilton was tasked to provide.

6.3.2 Expansion To Provide Global Viewpoint via USSTRATCOM

The effort that originated in the PACOM briefing initiated a two-year process that culminated in the drafting of an EW Initial Capabilities Document (ICD), approved by the Joint Requirements Oversight Council (JROC) in October 2009. [14] In the October 2009 JROC memorandum, General Cartwright asked USSTRATCOM and U.S. Joint Forces Command (USJFCOM) to develop a Terms of Reference (TOR) document for a study to assess the technical issues related to the EW problem, such as the "capability to effectively maneuver a waveform containing data within the spectrum to achieve the desired effect," and the organizational structure and management approach required to be responsive to emerging EMS threats.

The TOR document outlined the parameters of a study, led by USSTRATCOM in coordination with USJFCOM, to result in recommendations on organizational or management approaches that would enable the Department "to make timely and effective prioritized resource decisions in a congested, contested or hostile electromagnetic environment." [15] The final report is due to be provided to the JCS in Fall 2010 for consideration in bolstering the Department's ability to respond to emerging EMS threats.

6.3.3 Initial Meetings - Internal DoD Focus

Whereas USSTRATCOM will address how to strengthen DoD's capability to respond to emerging EMS environment threats, including recommending appropriate material and non-material courses of action, through the military chain (i.e., JROC), OSD additionally requires an organizational and structural leadership strategy for EMS control to not only integrate with the impending JROC-approved solution, but also to discreetly address various functions and responsibilities within OSD itself.

In parallel with the JROC efforts, the Secretary of Defense began raising questions about the broader implications of how emerging spectrum-related technologies impact DoD capabilities and investments. To this end, in September 2009, Zachary Lemnios, Director, Defense, Research and Engineering, created the EWTTF, inclusive of the Services and the Defense Advanced Research Projects Agency (DARPA), as well as leveraging expertise from USSTRATCOM. The intent was to assess current and projected technology and systems capabilities that are likely to emerge in the near- and far-term, and to provide recommendations to mitigate relevant vulnerabilities. [14]

The initial fact-finding and assessment work of the Task Force, which was focused on traditional DoD acquisition, development and intelligence, reinforced the assessments and observations provided during the December 2007 JCS Tank discussion (USPACOM) and the October 2009 JROC (USSTRATCOM):

- The global proliferation of commercial and dual use technologies (e.g., availability of high performance signal components and signal processors) gives rise to disruptive innovation, which drives new capabilities for our adversaries; and

- The Department requires leadership, management, or organizational structures to effectively assess the EMS technology environment, evaluate implications to national security objectives, and recommend appropriate solutions and courses of action.

6.4 EWTTF OUTREACH TO INDUSTRY, GOVERNMENT

The EWTTF assessment encompassed a whole-of-government approach, acknowledging a shift in emphasis of technology development toward commercial technology drivers and the need to look beyond traditional DoD resources. The Task Force's approach included extensive fact-finding that resulted from interactions with a wide range of leaders within and external to the Department to discuss the critical elements of an overarching DoD EMS environment control strategy and organizational approach.

6.4.1 Meetings with External Sources

The EWTTF met with a broad range of stakeholders external to the Department, including thought-leaders from across the commercial wireless and information technology sectors, the gaming industry, and academia to gain a deeper understanding of the current state of technology, emerging trends, and how the Department can support and be supported by the private sector with respect to EMS technology development. Meetings included representatives of hardware and software developers, equipment makers, carriers, technology developers, think-tanks, industry analysts, commercial wireless carriers, and defense industry experts. Topics covered included development of EMS strategy, DoD acquisition processes, evolving technology trends, forums for collaboration, spectrum control scenarios and concerns, security concerns associated with offshore manufacturing of electronic components, R&D requirements, basic science resources, and personnel and training needs. The list of meetings is shown in Appendix A. .

6.4.2 Results of Industry Consultations

The results of the Task Force's outreach to this cross-section of non-government EMS experts – which took place as part of in-person meetings, telephone interviews, and related follow-up activities – resulted in several key themes being raised.

1. **Off-shoring of EMS Tech Base**: The U.S. is no longer the dominant force in the manufacture of wireless network technologies, whose key components are increasingly produced by offshore manufacturing facilities.[10] The R&D and related innovation and intellectual capital that leads to the manufacture of technological innovations is also taking place more and more outside the U.S. This is a logical trend given several critical factors, including the explosion in R&D costs for highly sophisticated global networks, the move toward technological globalization, and the migration of manufacturing to regions with low-cost labor. On the other hand, this creates new sources of security concerns with respect to foreign competitors and adversaries.

   The diffusion of such technological capabilities raises broad issues for the global security of wireless networks, which are just now being understood, particularly because network concerns in this area initially centered on the implications for wireline networks.

2. **Outsourcing of Industrial Base/Knowledge Base**: The concentration of certain core network components in the hands of fewer firms – many of which are not U.S.-based – raises strategic considerations about a lack of diversity in the manufacturing base for EMS components. In addition, the technical knowledge base that provides a critical baseline for innovation also is increasingly globalized, facilitating the outsourcing of intellectual capital beyond U.S. shores. In the case of Huawei, these security implications are long-standing. Allegations of Huawei's close ties to Chinese government intelligence and military agencies have created security concerns that have given rise to stalled state-sponsored contracts in India and Australia, for example. (In the U.S., Huawei has secured infrastructure contracts with both Cox and Clearwire.)

   While other foreign owners of formerly U.S.-based technology manufacturing companies do not pose this kind of direct security threat, they still speak to a broader trend. In 2006,

[10] As an example, none of the major networking equipment manufacturers is based in the U.S. at this juncture. Huawei, a Chinese company, is poised to grab market share using technology transfers and low employment costs, and the remaining companies (Ericsson, Nokia, Siemens and Alcatel-Lucent) are European companies.

France-based Alcatel purchased Lucent, but only after reaching an agreement with the U.S. government on security issues. Similarly, while Sweden-based Ericsson does not raise the same security issues as Huawei does, its global reach is extensive, with equipment in more than 1,000 networks in 175 countries.

This issue does not just concern manufacturing. Companies such as Microsoft and Intel are increasingly situating major research facilities overseas, in places such as India and Israel. U.S. universities continue to attract large numbers of foreign students, but unlike in the past, many of those educated young people are returning to their native countries for high-tech jobs or further higher education. That "brain regain" movement back to developing countries is supported by (1) the rise of top-level universities in India, China and elsewhere, and (2) the leveling and distributing effect of the Internet, which allows information to be disseminated and used throughout the world.

The globalization of technology development, education, training and manufacturing, including in the area of EMS devices and systems, has led the U.S. to become a net importer of high-tech products. At the same time, there is also a general growth of awareness among companies that the Chinese government is persistently favoring its own national champions in a way not mirrored by other governments. Protectionist strategies are also a factor: The U.S. high-tech sector is raising concerns about “indigenous innovation” programs implemented in China last fall to establish a national catalog of products that receive major preferences for government procurement.

3. **U.S. Export-Import Rules as Barriers**: Several companies interviewed raised the issue of U.S. dual-use export rules and other trade policies. This issue already is familiar to the Department. The 2010 QDR highlighted the current export control system as a “relic of the Cold War” that impedes cooperation and technology sharing. Today’s system reflects an era when the U.S. was, as the QDR noted, “largely self-sufficient in developing technologies and when we controlled the manufacture of items from these technologies for national security reasons.” The President is directing a comprehensive review in this area to identify reforms to enhance U.S. national security, foreign policy, and economic security interests. In April 2010, Defense Secretary Robert Gates elaborated on why these proposed changes to the export control system are critical to the national security community. [16]

   The problem we face is that the current system – which has not been significantly altered since the end of the Cold War – originated and evolved in a very different era, with a very different array of concerns in mind. As a result, its rules, organizations, and processes are not set up to deal effectively with those situations that could do us the most harm in the 21st Century – a terrorist group obtaining a critical component for a weapon of mass destruction, or a rogue state seeking advanced ballistic-missile parts. Most importantly, the current arrangement fails at the critical task of preventing harmful exports while facilitating useful ones. To align with the President’s export control directive, Secretary Gates described reforms arrived at as part of an inter-agency coordination process and guided by a National Intelligence Council assessment of national security considerations: a single export control list, licensing agency, enforcement-coordination agency, and information-technology system.

4. **To Innovate, DoD Must Collaborate**: The economies of scale of U.S. commercial wireless networks versus military-specific EMS solutions mean the Department cannot afford to "go it alone" with stove-piped, DoD-centric systems. The potential for DoD to foster EMS technology R&D is eclipsed by the resources of the commercial tech world. This creates increased pressure for the Department to influence off-the-shelf technology at an early stage, by ensuring that warfighter considerations are reflected at the start of the design process for new systems. Among the tools in DoD's tool chest that were cited by private sector stakeholders (e.g., Vanu, Intel) during the Task Force's interviews was the ability to target R&D and S&T resources to technology at the initial stages of development (e.g., technology transfer from academia to commercialization). Moreover, Intel noted that the Department could be a more effective arbiter and market player in technology development if it consolidated its purchasing power in more integrated and strategic ways, rather than dispersing small amounts of investment across multiple, unrelated acquisition programs. With targeted spending, based on strategic guidance, the Department would gain the buying power leverage that its size advantage should otherwise confer on influencing the industrial base's technology development and supply chain issues.

5. **Making the Acquisition Process More Agile**: Challenges cited during stakeholder interviews (e.g., Boeing) with the current DoD acquisition process centered on a number of critical issues, including the Department's internal procedures, as well as Congressional funding authority.

6. **Fostering Innovation through Collaboration**: To better facilitate industry/government technology collaboration – and, in turn, development of COTS EMS technology that meets warfighter mission requirements – it was urged that DoD leadership take on a more proactive role. Several companies, including Lockheed Martin, Northrop Grumman and Boeing, identified the lack of a DoD strategy to guide their independent research and development efforts.

7. **Willingness of Private Sector/Academia to Engage**: Across most of these meetings, there was a strong focus on the willingness of the private sector actors, and related academic and research entities, to engage with the military in a dialogue on constructive solutions to EMS challenges. The Semiconductor Industry Association, which has a forum for public-private partnerships, suggested that this sort of dialogue might be useful. Verizon also cited the value of industry advisory groups such as the President's National Security Telecommunications Advisory Committee (NSTAC).[11] The Office of Science and Technology Policy (OSTP) and the Enduring Security Framework (ESF) were also identified as possible venues.[12]

[11] The NSTAC is a 25-year-old Federal advisory committee that brings together up to 30 CEOs from major private sector telecommunications companies, network service providers, information technology, finance, and aerospace companies. These leaders provide industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy. http://www.commscc.org/?page_id=112

[12] OSTP is the office within the White House that provides the President and his senior staff with data and advice on matters pertaining to technology and science policies. In September 2008, the Homeland Security Department and the Department of Defense launched the Enduring Security Framework as a joint effort to engage U.S.-based global companies to consider standards of practice for a secure supply chain, whether for software development, hardware manufacturing, employee vetting, or any other touch points along the production and distribution process.

8. **Need to Sustain a Culture of Innovation:** Stakeholders such as Google highlighted the extent to which it has created a culture of innovation that has enhanced the delivery of new technologies, citing elements of this approach as a possible model.

9. **Addressing Intellectual Property Challenges**: Some companies discussed issues involving intellectual property rights (IPR) infringement, which contributes to inequities faced by tech firms in the global marketplace. Certain countries represent “hot spots” for IPR concerns. More than 80 percent of IPR-infringing goods seized at the U.S. border, for example, are of Chinese origin. Such issues underscore the overarching challenge the U.S. faces as the manufacturing base for high-tech products shifts overseas.

10. **Making Sense of Data Deluge**: Several companies cited challenges associated with data analysis, assessment, and mining, as well as structured versus unstructured data. Google, IBM, Microsoft, and Jodange all raised the challenges of how to deal with increasing amounts of data in many forms (e.g., the dilemma of culling/managing useful information).

    One of the clearest implications of the interview results is that shifts and trends taking place across the global value chain for EMS-related technologies are having whole-of-society effects. Therefore, there is a clear need for a whole-of-government approach that addresses not only commercial manufacturing needs, but also the broad base of knowledge accumulation (i.e., higher education and S&T research and development), U.S. science and aeronautics agencies (i.e., the National Science Foundation and the National Oceanic and Atmospheric Administration), economic policies, law enforcement, and homeland security – as well as the Department of Defense.[13] The scope of such a strategic effort should embody a comprehensive and representative segment of industry and Federal users, manufacturers, and policy-makers in the EMS field.

    Based on DoD's EMS strategy articulated above, the next section explores all the ways in which a national EMS strategy should address current gaps and issues. It also discusses a framework for a national EMS strategy, based on a whole-of-government approach that recognizes and leverages current civilian pre-eminence in spectrum-based technology development and deployment.

7. TOWARD DEVELOPMENT OF A NATIONAL EMS STRATEGY

A national EMS strategy must involve multiple agencies within government, as well as all industries that produce EMS components and equipment, or that utilize EMS to provide services. Moreover, it must address the needs and requirements of all stakeholders through win-win solutions and approaches, avoiding zero-sum-game decision-making that picks winners and losers.

[13] The 2010 National Security Strategy document calls for such a national approach: "To succeed, we must update, balance, and integrate all of the tools of American power and work with our allies and partners to do the same." The document adds that "our economic institutions are crucial components of our national capacity and our economic instruments are the bedrock of sustainable national growth, prosperity and influence." (p. 14-15).

7.1 KEY PRINCIPLES

The key principles have been drawn from numerous interviews and analyses, both inside and outside the Department. They represent top-level lessons learned from the EWTTF, and they represent the core concerns of industry, other Federal agencies, and the Department itself. Each subsection below elaborates a key principle, as articulated in the findings:

7.1.1 Recognize the Prime Importance of EMS

Throughout the world, the evolution of spectrum-dependent industries over the last two decades has seen an unmistakable trend: the evolution of dominance by mobile technologies. The International Telecommunication Union (ITU) has documented the fact that mobile service minutes (both voice and data) overtook the number of landline minutes during the past decade. Increasingly, the vast preponderance of technical resources is being devoted to expanding the capacity of mobile networks to convey increasing amounts of data – in effect, eliminating most advantages that wireline networks have maintained over wireless ones.

This tsunami of commercial wireless technologies has been matched by a similar, if less monolithic, shift toward mobility in tactical military capabilities. With the advent of satellites, broadband tactical radios, and UASs, the military is also calling for exponential increases in wireless bandwidth.

The implications of these dual developments are clear, and they cannot be ignored by the U.S. military: the EMS environment will become increasingly vital for the success of the United States, technologically, economically, socially, and militarily. U.S. government policy must cogently address the growing prominence of wireless and EMS-based technologies – as it relates to both security and prosperity – or lose strategic ground to those governments that do.

7.1.2 Recognize the Ongoing Strengths of US Technological Capabilities

This report has focused on the views of U.S. and international companies regarding the relative disaggregation and leveling of technological leadership across the world. Indeed, by comparison with the latter half of the 20th century, the United States no longer retains a singular, dominant role in developing and deploying EMS technologies. The U.S. does, however, retain a vibrant and competitive set of industries that develop and manufacture EMS-related technologies. U.S.-based companies, along with multinational counterparts that maintain a significant presence here, reflect the importance of the U.S. market and the powerful force that the strong U.S. industrial base and economy retain in the world. U.S. higher education, moreover, is still regarded as the most effective, forward-looking, and innovative force in academia worldwide. Moreover, U.S. commercial labs, standards bodies, and marketing efforts still lead the world in many ways.

7.1.3 Recognize the Leadership of Commercial Technology Development

It is important for the Department to acknowledge, however, that many of these U.S. strengths lie outside the traditional military research and acquisition process. Commercial interests, not military priorities, are driving technology development in the United States and throughout much of the world. These commercial centers of excellence must be regarded as national assets and leveraged in a way that DoD has not done to date.

Taking advantage of commercial technology adoption prowess may well entail fundamental steps to reform acquisition policies and processes. This will not be a simple or non-controversial action by the Department – not only because of the vested interests in preserving the status quo, but also because of genuine security concerns. There must be a serious examination of the costs and benefits of retaining the current acquisition system, as opposed to loosening the criteria for rapid procurement of technologically strategic equipment. The Department should be frank about the risks and opportunities in obtaining equipment produced outside the United States whenever that equipment offers advantages or benefits in terms of differentiating technologies.

7.1.4 Recognize the Need for a Whole-of-Government Approach

As this report indicates, the relative de-emphasis of military EMS policies over the past two decades has resulted in nascent technology deficits throughout the military value chain, from the tactical up through the strategic. Moreover, it is becoming increasingly apparent that other countries, which have more integrated technology policies encompassing all spheres of national interest, are better positioned to leverage new dual-use technologies.[14]

Appropriate adjustments in the bifrucation of U.S. spectrum policy among civilian and military sectors should be considered to ensure that there are no nascent technology deficits throughout the military value chain and that national prosperity and national security are not impaired.

Without a national strategy, it may become increasingly difficult to coordinate a policy response to any deficits in technology development and adaptation. This may affect not only critical governmental goals, such as national defense and homeland security, but also the commercial development of critical infrastructures, such as wireless networks – which increasingly will become access networks of choice for the Internet. Therefore, it is increasingly difficult to segregate “military” EMS polices from “civilian” ones – and impossible to separate commercial and government approaches to technology development. What is needed is a coordinated, *whole-of-government* approach to EMS policy, encompassing not only commercial applications of wireless technology, but also public safety and defense applications as well. Anything less than an inter-agency approach risks long-term lack of cohesion and competitiveness across the entire range of spectrum uses. As the 2010 National Security Strategy states:

[14] The interviews EWTTF carried out for this report indicated a perception that Chinese and other foreign firms were able to make use of government support for development and incorporation of technologies. This viewpoint was echoed in congressional testimony by Wallace C. Gregson, ASD for Asian and Pacific Security Affairs, who told the House Armed Services Committee on 13 January 2010 that “we have been watching carefully as China has also embarked on a comprehensive effort to translate its increasing economic power into military power.” Among other components of Chinese military improvement, he noted “continued high rates of investment in its domestic defense and science and technology industries.” Mr. Gregson specifically mentioned new cyber-warfare technologies, directed-energy weapons and satellite communication jammers.

> The Executive Branch must do its part by developing integrated plans and approaches that leverage the capabilities across its departments and agencies to deal with the issues we confront. Collaboration across the government -- and with our partners at the state, local and tribal levels of government, in industry and abroad -- must guide our actions.

7.1.5 Recognize the Need for Change

Perhaps the primary requirement is a widespread recognition of a need for change. Interviews with company executives and government officials have indicated that this awareness exists and is growing throughout the commercial and governmental EMS communities. Numerous parties perceive the growing technological acumen of other nations' EMS-oriented R&D and commercial sectors. Many also perceive the more seamless integration of commercial and governmental action behind the growing relative power of U.S. rivals. Whether this power is explicit and non-threatening, as it is across Europe, or more implicit and unpredictable, as represented by China, the U.S. must awaken to the reality that it will require a societal effort to maintain leadership in the EMS technology sector and promote strategic, operational and tactical success in EMS security.

7.1.6 Recognize the Opportunity for Public-Private Partnerships

Bridging the counter-productive gap between commercial and public priorities will require judicious use of public-private partnerships to spotlight and develop critical EMS technologies. Universities, endowments, and "think tanks" can be the incubators for innovative partnerships, bringing their expertise, resources, and "good offices" to bear in creating neutral zones for technology creation. They can help to combine the rapid, non-bureaucratic, speed-to-market approach of the commercial sector with the national requirements and goals prompted by government relative to national security considerations.

7.2 BUILDING A STRATEGY

In constructing a strategy, it is useful to begin with a systematic analysis of realities and objectives in both the national and international spheres. The stages in this analysis can be described as follows:

1. Identification of assumptions – It is helpful to begin with a listing of a priori assumptions regarding the EMS control environment (across both domestic and international spheres);
2. Assessment of realities – The next step is a full analysis and assessment of whether objective realities correspond to those assumptions, or whether those assumptions must be recalibrated;
3. Listing of objectives – This step involves identifying the goals of the strategy, in terms of driving change from current realities to desired end states;
4. Analysis of the instruments of power and influence – This stage evaluates the tools that can be used to reach the objectives, including policies, processes, structures, etc.
5. Gap analysis – This stage explores what instruments of power/influence must be developed to reach the stated national international objectives.

This is a standard and useful approach for generating and refining strategy. As such, it should be considered as a potential analytical tool in articulating a national EMS control strategy.

7.3 THE EMS VALUE CHAIN

In formulating a national EMS control strategy, it also will be useful to articulate the areas in which EMS-related technologies function along a value chain (Figure 8), beginning with basic scientific research and development. For the military, this value chain proceeds to include more targeted research and system development, culminating in testing, training, and fielding of the new technologies. This subsection explores this value chain.

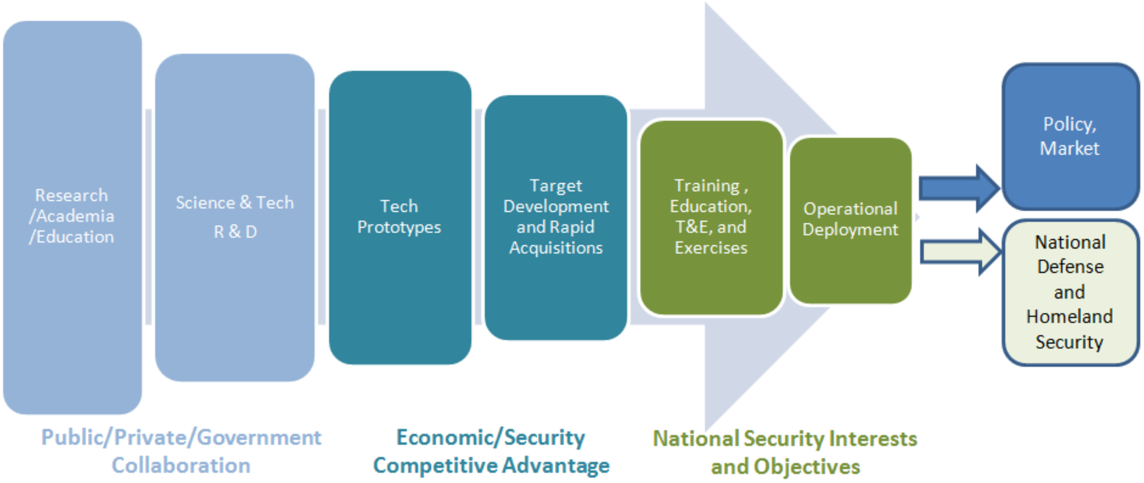

Research /Academia /Education
Science & Tech R & D
Tech Prototypes
Target Development and Rapid Acquisitions
Training , Education, T&E, and Exercises
Operational Deployment
Policy, Market
National Defense and Homeland Security
Public/Private/Government Collaboration
Economic/Security Competitive Advantage
National Security Interests and Objectives

Figure 8. "Value Chain" Development Strategy

7.3.1 Basic Research, Academia, and Education

At one end of the value chain is the foundation of basic technical knowledge engendered throughout U.S. society, by its institutions of education and research. These include K-12 schools, public and private, as well as colleges and universities, which accumulate both higher-education and research efforts.

Meetings with representatives of the National Science Foundation (NSF) indicated that American major research universities continue to be a beacon of excellence, drawing in students and researchers from around the world. This results in a net "brain gain," as many of these incoming individuals remain in the United States to pursue scientific and technical careers, within academia and in U.S. high-tech facilities. In addition, while the verdict regarding K-12 education is problematic, the nature of American higher education embodies an inherent advantage in that it promotes critical thinking, questioning of accepted hypotheses, and competition in research. Therefore, U.S. universities tend to be more dynamic and reward more entrepreneurial research than schools in other countries.

In addition, Federal involvement is necessary to provide high-level policy guidance to coordinate and provide a national strategy to boost critical teaching and research in science and engineering fields relating to EMS. This calls for a whole-of-government approach involving DoD, the Department of Commerce, the National Science Foundation, the Department of Education, and the universe of foundations, think tanks, universities and school districts that help build basic scientific and technical knowledge. Their efforts should be informed by market demand, articulated by U.S. and multinational corporations that develop and implement EMS-based technologies.

7.3.2 Science and Technology R&D

Moving down the value chain, there is a community devoted to focused S&T research and R&D. This will include university research labs, government research labs, and corporate research facilities. These categories may focus on EMS at different levels of abstraction, with universities specializing in more “pure” research and corporate R&D labs on the other end of the spectrum, developing specific technologies for new products that can be marketed for corporate profits.

Interviews with corporate representatives indicated that the amount of resources devoted to product development now dwarfs pure research and military-oriented R&D. This reflects the decisive shift toward condensed timelines and intense competition among international telecommunications equipment manufacturers. Product-focused S&T R&D will proceed according to the dictates of commercial market demand. Unless there is a national effort to mesh military technologies with market-oriented applied research, the commercial efforts will outpace pure research and military R&D, without providing any reference points or avenues for dual use. What is needed is a military capability to monitor and spotlight key technologies that can be adopted and adapted to differentiate EMS-related operations from those of military adversaries.

In essence, the traditional route of developing dual-use technology – by adapting military technologies to civilian uses – has been flipped. Commercial S&T R&D no longer can wait for adaptation of military-developed technologies, for it is proceeding too rapidly. The government, and particularly the military, must now adapt to the new paradigm, in which the commercial sector will develop dual-use technology, with the military adapting civilian components or even COTS equipment to military uses. This fundamental shift has not be recognized or applied in terms of a national policy or approach to S&T R&D.

7.3.3 Technology Prototypes

Meetings with equipment manufacturers revealed gaps in the ability of the Department to move from general or “pure” S&T R&D to the next stage of technology development: working prototypes of equipment This step is currently burdened by two existing challenges:

- The delays, resource drains, and inefficiencies of current contractor-based acquisition programs, with their attendant bureaucratic overheads; and
- A lack of sufficient capabilities and resources for large-scale modeling, simulation, and testing of components.

The shift from pure, or even applied, engineering to product development is one of the chief areas where commercial technology providers excel relative to military counterparts. Market-driven product development of advanced technology is essential to EMS-dependent equipment manufacturers; it can mean the difference between first-to-market advantage and market share loss. Reorganization of DoD business practices in this area, or the utilization of joint military-commercial development projects, should be considered as a national priority.

7.3.4 Targeted Development and Rapid Acquisitions

The U.S. military must be able to respond rapidly, with efficient allocation of resources, to immediate threats and new definitions of requirements. Current acquisition processes are not set up to respond rapidly, particularly in the area of EMS, which in the past has illustrated a gap between acquisitions and spectrum management communities. DoD must learn from commercial technology implementation processes in order to rapidly speed up procurement. This would include targeted development and alteration of commercial technologies, including purchase of COTS technologies where available. This would be enabled by increased incorporation of open source standards and an emphasis on interoperability across systems and Services. Security requirements should be built into equipment at early stages and should not be allowed to form a barrier to rapid acquisition of high-capability systems.

7.3.5 Training and Exercises

Once development and acquisition processes are reformed and accelerated, the Department must be able to respond with ramped up training and targeted exercises to integrate the equipment more rapidly into its force structures. This will require retention and even expansion of facilities, in CONUS, that are now utilized for training, testing, and operational exercises. Coordination with other government agencies, allies, and coalition partners will be crucial in accelerating the systems and processes needed for rapid development and training of new systems in operational modes.

U.S. military policy has consistently recognized the importance of maintaining a capability to "train as we fight." If the Department were to lose access to significant amounts of spectrum in CONUS regions, it could translate into the loss of sufficient geographic or spectral space in which to train and use new, adaptive EMS-based technologies. If these technologies cannot be tested and perfected in CONUS, they are not likely to be inserted successfully into operations outside CONUS. Combat should not be the first situation in which warfighters fully deploy their own EMS-dependent systems or encounter those of their enemies.

7.3.6 Operational Deployment

The last stage in the value chain model in terms of military capability is operational deployment, which brings the result of all other improvements into the realm of rapid technology insertion in operational environments. This is a major objective for DoD: translating national and strategic-level EMS-control improvements into the arena of the warfighter. At this stage, there must be dramatic and decisive coordination of operational, intelligence, and communications/spectrum management expertise to support rapid insertion. The entire goal of a national effort must culminate in a rapid and effective application of the latest EMS technology for use in the EMS battlespace. It must be done in a manner that is more efficient, effective, and rapid than the adversary can match or cope with. At stake is control over the battlefield, not only for delivery of information, but also for mobility, detection of enemy movements and action, electronic warfare, and uninterrupted command and control. EMS control is becoming increasingly critical to mission success.

As the value chain model illustrates, every element of the model is built upon a foundation of national policy and effort – cumulative actions that will benefit not only military readiness and execution, but also commercial competitiveness and market success. In other words, national security inherently rests upon national prosperity. In turn, national security also protects national prosperity, in a virtuous circle that allows for further strengthening along the entire value chain, from the halls of academia to the streets and alleys of Iraq and Afghanistan.

7.4 FINDING A FORUM FOR DIALOGUE

In order to realize the model, a whole-of-government and public-private approach will be necessary. This will depend upon institutions and agencies beyond the scope or authority of the Department of Defense. Leadership within the Department can, however, have a catalytic effect upon the remainder of government and private industry. Steps in building a consensus around a new national EMS strategy could resemble the following:

Step One: Build consensus around DoD leadership

Articulation of the need for a national strategy, and its internal DoD building blocks, would lead to high-level establishment of a coordination structure to serve as (a) a high-level DoD policy engine, (b) a point of contact for counterparts within government and industry, and (c) an oversight and guidance body for alignment of EMS-related activities and efforts within the Department.

Step Two: Coordinate with High-Level Executive Branch Leadership

To be successful on a whole-of-government scale, the effort to revitalize national EMS policy must be accepted and championed, on a sustained basis, at the White House. This would involve briefing and supporting the National Security Council and the Office of Science and Technology Policy, both of which will be critical players, along with the National Economic Council, in articulating and implementing new policies and directives throughout the Executive Branch. These entities will also be important in briefing the relevant committees of Congress, which must also be a leading player in articulating, implementing, and sustaining a national approach.

Step Three: Identify an Appropriate Forum for Public-Private Collaboration

There are several national forums that bring together corporate and government leaders at high levels to coordinate national policy discussions. These include the Commerce Spectrum Management Advisory Committee, the NSTAC and the Enduring Security Framework (ESF). Socialization of the policy may take significant effort and time, but acceptance among corporate leadership is vital to ensuring the success of any national strategy.

8. CONCLUSION

The work of the EWTTF has enabled policy-makers to draw some key conclusions:

- The EMS environment has become disparate, decentralized, and globalized – and no longer dominated by the United States.

- The U.S. retains advantages in the development of applications and software for wireless devices.

- The U.S. military cannot succeed with a "go-it-alone" strategy because the costs of EMS-dependent technology development, coupled with the required speed of development,, transcends its resources and capabilities.

- DoD must invest in technology areas of differentiation, adapting commercial technologies in a way that gives it advantages over other militaries.

- U.S. equipment manufacturers are increasingly frustrated with the DoD acquisition process and are seeking changes.

- The Department, and the entire U.S. government, have a role to play in counter-acting the current misunderstanding and minimizing of military requirements and contributions to the commercial wireless industry.

- Enlightened actors within the civilian technology community are poised to support and participate in a meaningful dialogue on these issues.

In order to secure both national prosperity and national security, the United States must undergo a paradigm shift in attitudes, policies, process, and structure with regard to EMS. The core of this paradigm shift is the mutual recognition, in both government and commercial entities, that revitalization of the Department's ability to serve as an engine and consumer of commercial EMS technology is vital to the achievement and sustainability of American pre-eminence in this sector. The Department cannot achieve this by itself; it requires a whole-of-government approach, both supporting and receiving support from U.S. and global industry. DoD must be part of the mainstream in developing and fielding technology, in order to keep pace with it.

DoD will lead the way in developing a new national consensus and strategy for capitalizing on America's intellectual and technological advantages. The United States must, and will, employ all of its resources to regain leadership in the EMS sphere, benefiting all of its citizens and its allies and leading the world toward a more prosperous, productive, and peaceful future.

This page intentionally left blank.

9. REFERENCES

1. DoD. *Electronic Warfare Initial Capabilities Document*, JROCM 177-09, DoD, Washington, DC: 30 October 2009.

2. DoD. *DoD Electronic Warfare Technology Task Force Final Report to OUSD AT&L/DDRE*, DoD, Washington, DC: 31 July 2010, SECRET/NOFORN.

3. Office of the Director of National Intelligence (ODNI). *The National Intelligence Strategy of the United States of America*, ODNI, Washington, DC: May 2009.

4. Gabriel, Caroline. *Rethink Wireless*, "Huawei paves way for Motorola bid? Seeking US government deal to allay security concerns," Rethink Wireless, UK: 6 April 2010, retrieved on 15 July 2010, www.rethink-wireless.com/2010/04/06/huawei-paves-motorola-bid.htm

5. Elder, Robert J., Lt Gen, USAF (Ret.). *21st Century Electronic Warfare*, Association of Old Crows, Alexandria, VA.

6. Defense Science Board (DSB). *Report of the Defense Science Board, 2008 Summer Study on Capability Surprise, Volume I: Main Report*, DSB, Washington, DC: September 2009, UNCLASSIFIED, retrieved on 15 July 2010 at www.acq.osd.mil/dsb/reports/ADA506396.pdf

7. Bibler, Jet, COL, Army. *The Nexus*, "Rebuilding the Army's Electronic Warfare Capability," U.S. Army Combined Arms Center, Fort Leavenworth, KS: 26 February 2009, retrieved on 15 July 2010 at http://usacac.army.mil/cac2/cew/nexus/NEXUS_VOL_2-2_-_COL_Bibler.pdf

8. Robb, Stephen C., Major, USMC. "Marine Corps Electronic Warfare--A Combat Power Multiplier," Global Security, Alexandria, VA: 1990, retried on 15 July 2010 at http://www.globalsecurity.org/military/library/report/1990/RSC.htm

9. Corbett, Blaise, and J. Partak. *CHIPS*, "The U.S. Navy's New Electromagnetic Pulse [EMP] Program, Resurrecting the Capability in a New World," CHIPS, Washington, DC: January-March 2010, retrieved on 15 July 2010 at www.chips.navy.mil/archives/10_jan/PDF/Navy_EMP.pdf"

10. DoD. *FY 96 Electronic Warfare Plan*, Office of the Under Secretary of Defense for Acquisition and Technology, Washington, DC: April 1995, retrieved on 15 July 2010 at http://www.dod.gov/pubs/foi/reading_room/790.pdf

11. Markoff, John. *The New York Times* "Georgia Takes a Beating in the Cyberwar with Russia," New York Times, New York, NY: 11 August 2008, retrieved on 15 July 2010 at http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/

12. DoD. *Quadrennial Defense Review Report*, DOD, Washington, DC: February 2010.

13. JROC Memorandum for Commander, USSTRATCOM, Commander, USPACOM, JROCM 177-09, 30 Oct 2009, approving an EWICD and designating STRATCOM as the lead component to develop a TOR and conduct the EW Organization study.

14. DoD. Control of the Electromagnetic Environment, Terms of Reference, DoD, Washington, D.C.: 17 November 2009, UNCLASSIFIED, FOR OFFICIAL USE ONLY.

15. DoD. DoD *Electronic Warfare Technology Task Force,* Director, Defense Research and Engineering, Washington, D.C.: 28 September 2009.

16. Gates, Robert. *Export-Control Reform, Business Executives for National Security* (Complete Text of Speech), DoD, Washington, D.C.: 20 April 2010, retrieved on 15 July 2010 at http://www.djacobsonlaw.com/2010/04/complete-text-of-secretary-gates-export.html.

10. ACRONYM LIST

COTS	Commercial-Off-The-Shelf
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
EMS	Electromagnetic Spectrum
EW	Electronic Warfare
EWTTF	Electronic Warfare Technology Task Force
GPS	Global Position System
IED	Improvised Explosive Device
IP	Intellectual Property
IPR	Intellectual Property Rights
JIEDDO	Joint IED Development Office
JROC	Joint Requirements Oversight Council
NSTAC	National Security Telecommunications Advisory Committee
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OSD	Office of the Secretary of Defense
QDR	Quadrennial Defense Review
R&D	Research and Development
RFID	Radio Frequency Identification Devices
ROMO	Range of Military Operations
S&T	Science and Technology
TOR	Terms of Reference
USJFCOM	U.S. Joint Forces Command
USPACOM	U.S. Pacific Command

USSTRATCOM	U.S. Strategic Command

A. LIST OF INTERVIEWS

I. Government Intelligence Agencies

- Central Intelligence Agency
- Defense Intelligence Agency
- Federal Bureau of Investigation
- Missile and Space Intelligence Center
- National Air and Space Intelligence Center
- National Ground Intelligence Center
- National Security Agency
- Office of Naval Intelligence

II. Industry

- Alcatel Lucent
- BAE
- Boeing
- Cisco
- Ericsson
- Google
- IBM
- Gaming Industry
- Intel Corp
- Jodange
- Lockheed Martin
- Microsoft
- Motorola
- Northrop Grumman
- Orbital
- Qualcomm
- Raytheon
- Rockwell Collins
- SPEC
- Semiconductor Industry Association
- Vanu
- Verizon

III. Academic, Technology and Policy Institutions

- Academy of Sciences (Disruptive Tech, Gaming)
- Association of Old Crows
- Brookings Institution

- CNA
- Center for Strategic and International Studies
- GTRI
- Highlands Group
- HIS International, L.C.
- Institute for Defense Analyses
- Johns Hopkins University-Applied Physics Laboratory
- MITRE Corporation
- National Defense University
- Naval War College
- Naval Postgraduate School
- National Science Foundation
- New America Foundation
- Purdue University
- RAND
- Sandia National Labs
- University of Hawaii
- Washington Analysis

IV. Joint Organizations

- Joint Functional Component Command - Network Warfare
- Joint Staff
- United States Central Command (J3, J6, J8)
- United States European Command (J3)
- United States Joint Forces Command
- United States Northern Command (J3, J8)
- United States Pacific Command
- United States Southern Command (Innovation, Partnering, Strategy/Policy/Plans)
- United States Special Operations Command (J3, J8)
- United States Strategic Command

V. Service Organizations

- Air Force Scientific Advisory Board
- Joint Strike Fighter, Joint Program Office
- Joint IED Defeat Organization
- N89
- Naval Air Systems Command
- Naval Surface Warfare Center Crane SAF Red Team
- Navy Warfare Development Command
- PMR-51 (Red Team)
- Space and Naval Warfare Systems Command
- Space Protection Program

VI. Other Government Agencies

- US Department of Commerce
- US State Department
- US Department of Homeland Security

VII. International

- Australia
- North Atlantic Treaty Organization
- Singapore Embassy in U.S.
- Singapore International Risk Assessment and Horizon Scanning Symposium
- United Kingdom

B. CURRENT POLICY PLAYERS IN THE EMS CONTROL ENVIRONMENT

Policy around EMS control requires cooperation and coordination of a wide range of stakeholders both in the U.S. and abroad. These stakeholders represent military, government, and international perspectives to handle the complex technical, regulatory, legal, and sovereignty challenges that EMS control touches.

Military agencies are on the front line in operationally enabling EMS control, both offensively and defensively. They are in the best position to understand operational requirements and how to meet them through the acquisition process. In the U.S., the Department of Defense's Defense Spectrum Organization (DSO) and the OSD (via the Networks and Information Integration/DoD Chief Information Officer) have primary oversight of policy and operations functions. OSD' s Acquisition Technology & Logistics directorate, the DARPA and the Combatant Commands (COCOMS) are also involved in varying aspects of EMS control.

At an operational level, the Joint Frequency Management Office, Army Spectrum Management Office, Navy-Marines Corps Spectrum Center, and Air Force Frequency Management Agency provide technical support in planning and utilizing EMS assets for deployments and other operations. The Joint Staff J-6 Command, Control, Communications, & Computer Systems staff plays a key coordination role.

Militaries in the U.S. and other democratic nations, however, are subject to oversight by non-military executive and legislative bodies. These government branches have policymaking authority and set EMS priorities along a hierarchy of priorities. The White House, Congress, and U.S. spectrum regulators have responsibilities that intersect in the policy space. There are two U.S. spectrum regulators: the National Telecommunications and Information Administration (NTIA), which is a division of the Commerce Department, and the Federal Communications Commission (FCC), which is an independent agency. NTIA regulates the spectrum usage of Federal government agencies, while the FCC regulates usage by other entities, including commercial companies and state and local governments. Both NTIA and FCC have sub-divisions that are responsible for EMS policy, regulation and technical issues. Further, even within the Federal government, EMS control policies are influenced by multiple non-military entities, such as the Department of Homeland Security and the Federal Aviation Administration.

Internationally, the International Telecommunication Union (ITU), regional communications groups, foreign alliances, and foreign military agencies all play various roles in addressing various areas of EMS policy.

C. DISTRIBUTION LIST

External	**No. of Copies**
To be determined by STRATCOM	TBD
Internal	
Mike Williams (.pdf)	1
LTC Laughlin(.pdf)	1
Robert Schneider (.pdf)	1
Robert Lynch (.pdf)	1
Tim Trusner (.pdf)	1
John Alden (.pdf)	1
Fred Wentland (.pdf)	1

This page intentionally left blank.